UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERÍA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

TESIS

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DE PIURA SEGÚN LA NTP ISO/IEC 27001"

PRESENTADO POR:

BACH. IVÁN ALEXANDER VEGAS VARONA

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO INFORMÁTICO

LÍNEA DE INVESTIGACIÓN:

INFORMÁTICA, ELECTRÓNICA Y TELECOMUNICACIONES

SUB LÍNEA DE INVESTIGACIÓN:

COMPUTACIÓN

PIURA, PERÚ

2019

UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERÍA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

TESIS

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DE PIURA SEGÚN LA NTP ISO/IEC 27001"

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO INFORMÁTICO

LÍNEA DE INVESTIGACIÓN:

INFORMÁTICA, ELECTRÓNICA Y TELECOMUNICACIONES

SUB LÍNEA DE INVESTIGACIÓN:

COMPUTACIÓN

BACH. IVÁN ALEXANDER VEGAS VARONA
TESISTA

ING. TEOBALDO LEÓN GARCÍA, MSc.
ASESOR

DECLARACIÓN JURADADE ORIGINALIDAD DE LA TESIS

Yo: Iván Alexander Vegas Varona, identificado con DNI N°46858430, Bachiller de la Escuela Profesional de Ingeniería Informática, de la Facultad de Ingeniería Industrial y domiciliado en calle Los Ángeles 631 del Distrito Castilla, Provincia Piura, Departamento Piura.Celular:972987435. Email:ivegasv@hotmail.com

DECLARO BAJO JURAMENTO: que la tesis que presento es original e inédita, no siendo copia parcial ni total de una tesis desarrollada, y/o realizada en el Perú o en el Extranjero, en caso contrario de resultar falsa la información que proporciono, me sujeto a los alcances de lo establecido en el Art. N° 411, del código Penal concordante con el Art. 32° de la Ley N° 27444, y Ley del Procedimiento Administrativo General y las Normas Legales de Protección a los Derechos de Autor.

En fe de lo cual firmo la presente.

Piura 18 de julio del 2019.

.....

Bach. Iván Alexander Vegas Varona

DNI N°46858430

Artículo 411.- El que, en un procedimiento administrativo, hace una falsa declaración en relación con hechos o circunstancias que le corresponde probar, violando la presunción de veracidad establecida por ley, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.

Art. 4. Inciso 4.12 del Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales –RENATI Resolución de Consejo Directivo N° 033-2016-SUNEDU/CD

UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERÍA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

LOS QUE SUSCRIBEN, MIEMBROS DEL JURADO CALIFICADOR

CERTIFICAN LA APROBACIÓN DE LA TESIS:

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DE PIURA SEGÚN LA NTP ISO/IEC 27001"

Ing. Carmen Zulema Quito Rodríguez, MSc.
Presidente

Ing. Luis Alberto Calderón Pinedo
Secretario

Ing. Arturo Sandoval Rivera
Vocal

UNIVERSIDAD NACIONAL DE PIURA
FACULTAD DE INGENIERÍA INDUSTRIAL
DECANATO

ACTA DE EVALUACIÓN Y SUSTENTACIÓN DE TESIS

Expediente N° 1148 / 2015

Los miembros del Jurado Calificador Ad-Hoc de la Sustentación de Tesis nombrado con Resolución N° **016-CF-FII-UNP-16** de fecha 15/01/2016 que suscriben, se reunieron en acto público en la sala de exposiciones de la Facultad de Ingeniería Industrial de la Universidad Nacional de Piura, el día **30 de Mayo del 2019** a las **11:00 am**, para evaluar la defensa de la Tesis titulada **"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS ACADÉMICOS DE LA UNIVERSIDAD NACIONAL DE PIURA BASADO EN LA NTP ISO/IEC 27001"**, presentada por el Bachiller **IVAN ALEXANDER VEGAS VARONA** y asesorado por el **MG. TEOBALDO LEÓN GARCÍA** .

FACULTAD DE INGENIERÍA INDUSTRIAL
Dirección de Investigación
UNP

Después de haber calificado el Informe Final de la Tesis, escuchada la sustentación y las respuestas a las preguntas formuladas por el Jurado, se le declara ...Aprobada... para optar el Título de **INGENIERO INFORMÁTICO** con el puntaje de ..61.. que corresponde al calificativo de ...BUENO...

Jurado / Calificación	Presidente	Secretario	Vocal	Puntaje Promedio
Documento (Max 60 puntos)	34	34	34	34
Sustentación (Max 40 puntos)	27	27	27	27
PUNTAJE TOTAL				61

En consecuencia, el sustentante queda en condición de recibir el Título Profesional que se indica, conferido por el Consejo Universitario de la Universidad Nacional de Piura de conformidad con las Normas Estatutarias y la Ley Universitaria en vigencia.

Ciudad Universitaria, 30 de Mayo del 2019

MSc. CARMEN ZULEMA QUITO RODRÍGUEZ	Ing. LUIS ALBERTO CALDERÓN PINEDO	Ing. ARTURO SANDOVAL RIVERA
PRESIDENTE	**SECRETARIO**	**VOCAL**

DEDICATORIA

A Dios por darme las fuerzas para seguir adelante y ayudarme a alcanzar con fe, esfuerzo y dedicación mis metas.

A mis padres, quienes me han brindado su apoyo de manera incondicional y en todo momento me alentaron a continuar en la lucha de concretizar de este sueño compartido con comprensión y amor

AGRADECIMIENTOS

A los Ingenieros Víctor Benites Canessa, Jorge Sandoval Rivera, Carlos Correa García, Anthony Távara y Teobaldo León García por su apoyo, orientación y paciencia durante este tiempo en la realización de mi investigación, para de esta manera optar por un triunfo más en mi vida profesional como es mi Título Profesional.

.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

La Universidad Nacional de Piura tiene la necesidad de proteger sus activos e información frente amanezas, que son importantes y cruciales para el desarrollo de sus actividades académicas. De ahí que la presente investigación tiene como objetivo diseñar un Sistema de Gestión de Seguridad de la Información, para los Procesos Académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001, con el fin de garantizar la confiablidad, integridad, disponibilidad y auditabilidad de la información.

Para ello, se realizaron varias reuniones con el personal estratégico, operativo del Centro de Informática y Telecomunicaciones y Facultades que permitió definir el alcance del Sistema de Gestión de Seguridad de la Información e identificar y valorar los activos de la institución. Posteriormente se analizó la Situación Actual de Seguridad de los procesos académicos y evaluó los riesgos a los cuales estan sometidos los activos, siguiendo la metodología de la NTP ISO/IEC 27001.

Los resultados de esta investigación indican que existen políticas y controles mínimos implementados pero estos no están documentados, un bajo porcentaje de cumplimiento de la seguridad de la información, y un alto valor de criticidad de la información y activos en los procesos académicos. A partir de esto se diseñó el Sistema de Gestión de Seguridad de la Información, con los controles propuestos, basado en la NTP ISO/IEC 27001.

Palabras Claves: Activos informáticos, Seguridad de la información, Procesos académicos, Políticas de seguridad de la información, NTP ISO / IEC 27001.

ABSTRACT

The National University of Piura has the need to protect its assets and information against threats, which are important and crucial for the development of its academic activities. However, the ignorance of these issues by the authorities has caused that the necessary measures are not taken.

Due to this, the present investigation has like objective Designing a System of Management of Security of the Information, for the Academic Processes of the National University of Piura according to the NTP ISO / IEC 27001, in order to guarantee the reliability, integrity, availability and auditability of information.

To this end, several meetings were held with the strategic, operational personnel of the Center for Information Technology and Telecommunications and Faculties, which made it possible to define the scope of the Information Security Management System and identify and assess the assets of the institution. Subsequently, the Current Security Situation of the academic processes was analyzed and the risks to which the assets are subject were evaluated, following the methodology of the NTP ISO / IEC 27001.

The results of this research indicate that there are minimal policies and controls implemented but these are not documented, a low percentage of compliance with information security, and a high criticality value of the information and assets in the academic processes. Based on this, the Information Security Management System is designed, with the proposed controls, based on the NTP ISO / IEC 27001.Keywords: design, active, Security of the information ,processes, information security policies, NTP ISO / IEC 27001.

Keywords: IT assets Security of the information, Academic processes, Information security policies, NTP ISO / IEC 27001.

INTRODUCCIÓN

La información, en todas sus formas (automatiza o no automatizada, formalizada o no formalizada, pública o reservada, etc.), es uno de los principales activos de cualquier organización, necesario para el normal funcionamiento y la consecución de los objetivos que tenga marcados. (ISO 27001:05, 2005).

La seguridad puede ser afectada a través de cualquiera de sus tres componentes: el uso indebido de la tecnología, la falta de procesos de planificación de seguridad o el desconocimiento de las personas acerca de las distintas medidas de seguridad informática.

La seguridad de la información se encarga de la búsqueda de la preservación de la confidencialidad, integridad y disponibilidad de la información, es decir, buscar protegerla tanto de ataques físicos, tales como robos o incendios, como de ataques cibernéticos, tales como el aprovechar vulnerabilidades de los sistemas de información. (NTP ISO/IEC 17799)

Es por esta razón que las instituciones han comenzado a tomar conciencia y a proteger aquellos recursos de información que son cruciales para ellos, las distintas organizaciones buscan asegurar la integridad, confidencialidad y disponibilidad de la información.

Un Sistema de la Seguridad de la información es esencial para sobrevivir en un mercado tan competitivo, aún más si se trata de una Institución que está alineada a los avances científicos, tecnológicos y educativos que son imprescindibles para su acreditación a nivel nacional e internacional, como lo es la Universidad Nacional de Piura a la que luego denominaré UNP ya que permite asegurar los niveles de confiabilidad, integridad, disponibilidad y auditabilidad de la información académica, evitando mayores costos operativos, baja productividad, pérdida de información y de dinero, logrando de esta manera asegurar la continuidad del negocio con una seguridad aceptable bajo los estándares internacionales.

Por tal motivo un Sistema de Gestión de Seguridad de la Información permite a las instituciones poder identificar los riesgos que atenten contra sus recursos y tratar de mitigarlos, implementando ciertos controles capaces de brindar un nivel aceptable de seguridad.

CAPÍTULO I: ASPECTOS DE LA PROBLEMÁTICA

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA.

En la actualidad, los sistemas que se utilizan para almacenar, procesar y transmitir información se encuentran en toda clase de instituciones de diferentes rubros y funciones. Los sistemas de información se han vuelto más complejos debido a la globalización que tiene por consecuencia que las distancias geográficas ya no supongan un obstáculo. De esta forma existe una cantidad cada vez mayor de personas que tienen acceso a información que podría ser crítica para las diferentes empresas e instituciones en las que trabajan.

Adicionalmente a este riesgo interno, siempre se tiene presente el riesgo que supone la fuga de información sensible ya sea por medio de personas que cuentan con acceso a dicha información, como por terceros que han accedido a ella mediante algún mecanismo de ataque. (NTP ISO/IEC 27001)

Si bien se cuenta con una serie de normas estándar internacionales, publicadas por la Organización Internacional de Normalización (ISO), en el Perú se han definido leyes alineadas a éstos para que puedan ser aplicadas al contexto de las empresas existentes en el país en cuanto a la gestión de la información utilizada por las instituciones públicas. (NTP ISO/IEC 17799)

En nuestro país, desde hace más de diez años, las políticas del gobierno han ido recomendando una adecuada gestión de la seguridad de la información con resoluciones ministeriales tales como la N° 224-2004-PCM en la que aprueban el uso obligatorio de la NTP ISO/IEC 17799:2004 en las entidades públicas referente a las buenas prácticas para gestionar la seguridad de la información (NTP ISO/IEC 17799)

Adicionalmente, el marco legal de nuestro país obliga a las entidades públicas, pertenecientes al Sistema Nacional de Informática, el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basándose en la Norma Técnica Peruana (NTP) – ISO/IEC 27001:2008 mediante la resolución ministerial N° 129-2012-PCM emitida el 23 de mayo del 2012.

Como entidad pública la Universidad Nacional de Piura se encuentra sujeto a las regulaciones establecidas por el estado en diferentes aspectos relacionados con las actividades que realiza, es así que requiere contar con un Sistema de Gestión de la seguridad de la información, ajustado a las normas vigentes.

Sin embargo, el desconocimiento de estos temas por parte de la alta dirección de dicha casa de estudios, ha ocasionado que no se tomen las medidas necesarias para asegurar el resguardo de la información, que propone la Norma Técnica.

Actualmente la Universidad Nacional de Piura cuenta con políticas y controles de seguridad de la información minimos para realización de sus actividades académicas pero éstas no se encuentran documentadas. Sin embargo debido a la sensibilidad y criticidad de la información y activos, no son suficientes para reducir los riesgos en el manejo, almacenamiento y distribución de la información contenida en los diversos sistemas informáticos, equipos de cómputo, procesos con falla de seguridad, perjudicando la integridad, confiabilidad y disponibilidad de la información.

Los sistemas de información para el registro y control académico, de dicha casa de estudios , al no contar con políticas de seguridad implementadas y documentadas, podría ocasionar alteraciones selectivas como adulteración de datos académicos (notas, datos de créditos y cursos aprobados, etc.), sabotaje a los servidores, manipulación de los sistemas de información por personas ajenas al proceso o instituciones entre otras.

Para esta investigación se realizó un enfoque en la seguridad de la información para los procesos académicos, que son matrículas, inscripciones por cursos, emisión de actas, registro de notas. En estos procesos está implicada información y equipos informáticos que son de gran importancia para la institución, por ejemplo: registro de notas, actas, sistemas académicos, servidores, donde se almacena toda la data de los sistemas de la institución.

En ese sentido, surge la necesidad de un Diseño de un Sistema de Gestión de Seguridad de la Información, según la NTP ISO/IEC 27001, para mitigar las distintas modalidades de ataques, casos de fuga de información, modificación indebida de datos, accesos indebidos a los sistemas informáticos entre otros, ajustándose a la normativa a la cual está sujeta la institución para cubrir las necesidades de seguridad que actualmente carece dicha casa de estudios y que en un futuro pueda servir como referencia a otras universidades y estamentos públicos y privados.

1.2. FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN.

1.2.1. Problema General

¿Cómo diseñar un Sistema de Gestión de Seguridad de la Información de los procesos académicos de la Universidad Nacional de Piura, basado en la aplicación de la NTP ISO/IEC 27001?

1.2.2. Problemas específicos

- ¿Cuál es la situación actual de los sistemas de gestión de la información de los procesos académicos en la Universidad Nacional de Piura?
- ¿Cuáles son los procesos académicos que requieren modelamiento?
- ¿Cuál es la valorización de los activos de la información encontrados?
- ¿Cuáles son los riesgos de los activos encontrados?
- ¿Qué controles requieren ser elaborados para mitigar los riesgos encontrados?

1.3. JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN

Actualmente los constantes cambios tecnológicos, el manejo de la seguridad de información a todo nivel; se convierte en un problema grave y tiende a ser motivo de descuido en las instituciones cuando no se le brinda el control y tratamiento apropiado. Si no se identifican los problemas medulares, se ignora los riesgos que llevan a mantener la confiabilidad, integridad y disponibilidad de la información.

La inexistencia de políticas que coadyuven a proteger y controlar a través de una implementación, con el fin de brindar seguridad a la información en los procesos académicos de la Universidad Nacional de Piura, es preocupante.

Por esta razón la presente investigación, se tuvo como objetivo fundamental diseñar un Sistema de Gestión de Seguridad de la información que proporcione mejoras mediante controles y sus actividades correspondientes, que permitan un ambiente adecuado de seguridad alineado a los estándares de la NTP ISO/IEC 27001, para garantizar la confiabilidad, integridad, disponibilidad y auditabilidad de la información proveniente de los procesos académicos de la Universidad Nacional de Piura con el fin de proteger los activos frente a amenazas y riesgos que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzar los objetivos institucionales.

1.4. OBJETIVOS.

1.4.1. General

DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION PARA LOS PROCESOS ACADEMICOS DE LA UNIVERSIDAD NACIONAL DE PIURA, BASADO EN LA NTP ISO / IEC 27001.

1.4.2. Específicos

- Analizar la situación actual de la Seguridad de la información en los procesos académicos.
- Modelar los Procesos Académicos del problema de estudio.
- Valorar los activos de información de dichos procesos.
- Evaluar los riesgos a dichos activos.
- Elaborar los controles asociados a los riesgos identificados.

1.5. DELIMITACIÓN DE LA INFORMACIÓN

En este proyecto se optó por elegir siete de los catorce dominios con sus respectivos controles de la NTP ISO/IEC 27001, los cuales son:

1. Política de Seguridad.
2. Aspectos Organizativos de la seguridad de Información.
3. Seguridad Ligada a los Recursos Humanos
4. Gestión de Activos.
5. Control de Accesos.
6. Seguridad en la Operativa.
7. Seguridad en las Telecomunicaciones.

Del mismo modo para los procesos académicos de la Universidad Nacional, se seleccionó siete procesos académicos, entre ellos dos del Centro de Informática y Telecomunicaciones (CIT). A continuación se mencionan:

1. Calendarización Académica.
2. Programación Académica por semestre.
3. Proceso de Inscripción por cursos.
4. Proceso de Modificación de notas.
5. Proceso de Generación de Actas.
6. Procesos de Desarrollo de Sistemas.
7. Procesos de Soporte Informático.

La inclusión de estos procesos se debió a que se identificó una escasa gestión de controles, políticas no documentados e implementadas en aquellos dominios, generando vulnerabilidades y riesgos en los procesos mencionados en materia de seguridad; donde se maneja activos sensibles y claves para la gestión académica, como por ejemplo: sistemas académicos, servidores, registro de notas, registro de inscripción de cursos, registro de emisión de actas; etc. , procesos que son necesarios para el correcto funcionamiento académico de la Universidad Nacional de Piura.

CAPÍTULO II: MARCO TEÓRICO.

2.1. ANTECEDENTES DE LA INVESTIGACIÓN.

ERICK TORRES REQUENA (2015), presentó su proyecto de tesis: **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION PARA LA EMPRESA "AUTOBOUTIQUE CENTRO REAL S.A.C"- TALARA,** el propósito de esta tesis fue crear un plan de seguridad, donde se definen los lineamientos de la planeación, el diseño e implantación de un modelo de seguridad con el objetivo de establecer una cultura de seguridad en la organización. Este plan tiene como objeto proteger la información y los activos de la organización, tratando de conseguir la confidencialidad, integridad y disponibilidad de los datos; y las responsabilidades que debe asumir cada uno de los empleados de la organización.

La presente investigación brindó apoyo en la consideración del diseño del Sistema de Gestión de Seguridad de la Información, el cual se basó bajo la misma Norma ISO 27001 de la investigación, por lo que permitió gestionar la seguridad de sus activos con el objetivo de darles un tratamiento adecuado.

Vasco Rodrigo Talavera Álvarez (2015) en su proyecto de tesis: **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA ENTIDAD ESTATAL DE SALUD DE ACUERDO A LA ISO/IEC 27001:2013** , se centró en los procesos institucionales referentes al área de admisión de pacientes, limitando el alcance, siguiendo la metodología PDCA, que solicita los requerimientos necesarios para llevar a cabo un buen análisis y diseño de un Sistema de Gestión de seguridad de Información

Para este diseño utilizaron las Normas ISO 27001 que menciona los requerimientos para realizar un Sistema de Gestión de Seguridad de Información, ISO 27002, menciona el conjunto de objetivos de control y controles que pueden ser aplicados para el tratamiento del riesgo, ISO 31000, es un estándar internacional que sirve como referencia a la evaluación y gestión de riesgos y ISO 27779 es norma que aplica los conceptos contenidos en la norma 27002 al entorno de las instituciones de salud. Además utilizo la herramienta informática como Business Process Management BPM 2.0 para simular los procesos de la Institución.

La presente investigación sirvió como orientación en el diseño del Sistema de Gestión de Seguridad de la Información; el cual considera a la Norma ISO/IEC 27001:2013, planteando mejoras a la seguridad actual, reduciendo los riesgos que conlleva las actividades propias de la institución.

EDWIN ARNULFO SAAVEDRA NAVARRO (2011), en su tesis para optar el grado académico de maestro EN: INGENIERIA DE SISTEMAS, titulada "**EVALUACION DE LA SEGURIDAD DE LA INFORMACION EN LA UNIVERSIDAD NACIONAL DE PIURA",** El presente trabajo de investigación tiene como objetivo evaluar la situación actual en el tratamiento de la seguridad de la información que presenta la Universidad Nacional de Piura, para ello se realizó el análisis y evaluación de riegos con el fin de revelar las vulnerabilidades y amenazas a las que está expuesto el activo de información, en términos de ausencia, insuficiencia o inconsistencia de los controles de seguridad y procesos, con el fin y/o propósito de diseñar opciones de tratamiento adecuado y estrategias que permitan mitigar la ocurrencia de riesgos que podrían afectar dichos activos.

Dicha investigación brindó un marco referencial sobre la situación actual de seguridad informática y va dirigida específicamente al objeto de estudio de la presente investigación , fue el motivo de su selección brindando el soporte en relación a los 3 pilares en la seguridad de la información como son la; confidencialidad integridad y disponibilidad de sus activos de información.

CARLOS A. CORREA GARCÍA (2011), en un estudio de investigación titulado**: "ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD**" DE LA INFORMACIÓN OPERACIONES OLEODUCTO, tiene como objetivo Identificar, analizar y evaluar los riesgos de Seguridad de la Información asociados a los activos de información de Operaciones Oleoducto, con el fin de estimar los niveles de exposición al riesgo y tener un sustento para seleccionar las alternativas de tratamiento del riesgo e implementar los controles orientados a mitigar los riesgos.

La presente investigación apoyó en el Análisis y Evaluación de Riesgos y el diseño de controles orientados a mitigar dichos riesgos.

2.2. BASES TEÓRICAS.

2.2.1. Historia de la Universidad Nacional de Piura.

El 03 de marzo de 1961 se promulga la Ley N° 13531, por la cual se crea la Universidad Técnica de Piura, en virtud a la Ley Universitaria N° 23733, desde 1984 asume la nominación de Universidad Nacional de Piura. La responsabilidad social compromete a la UNP con las demandas de la comunidad regional y nacional; ello ha generado un desarrollo orgánico en el aspecto académico, el cual se expresa en la constitución de 14 Facultades con 31 Carreras Profesionales y a las que se adscriben 44 Departamentos Académicos, una Escuela de Postgrado con 24 Programas de Maestría y 12 Programas de Doctorado; una Escuela Tecnológica Superior con 05 Carreras Técnicas; un Colegio de Aplicación que cuenta con los niveles de Inicial, Primaria y Secundaria a la fecha.(Estatuto UNP,2014)

2.2.2. Función Operacional de la Universidad Nacional de Piura.

Para Rosales G. (2008) la Universidad Nacional de Piura, vista como una función operacional, se puede representar como aparece en el siguiente gráfico 2.1:

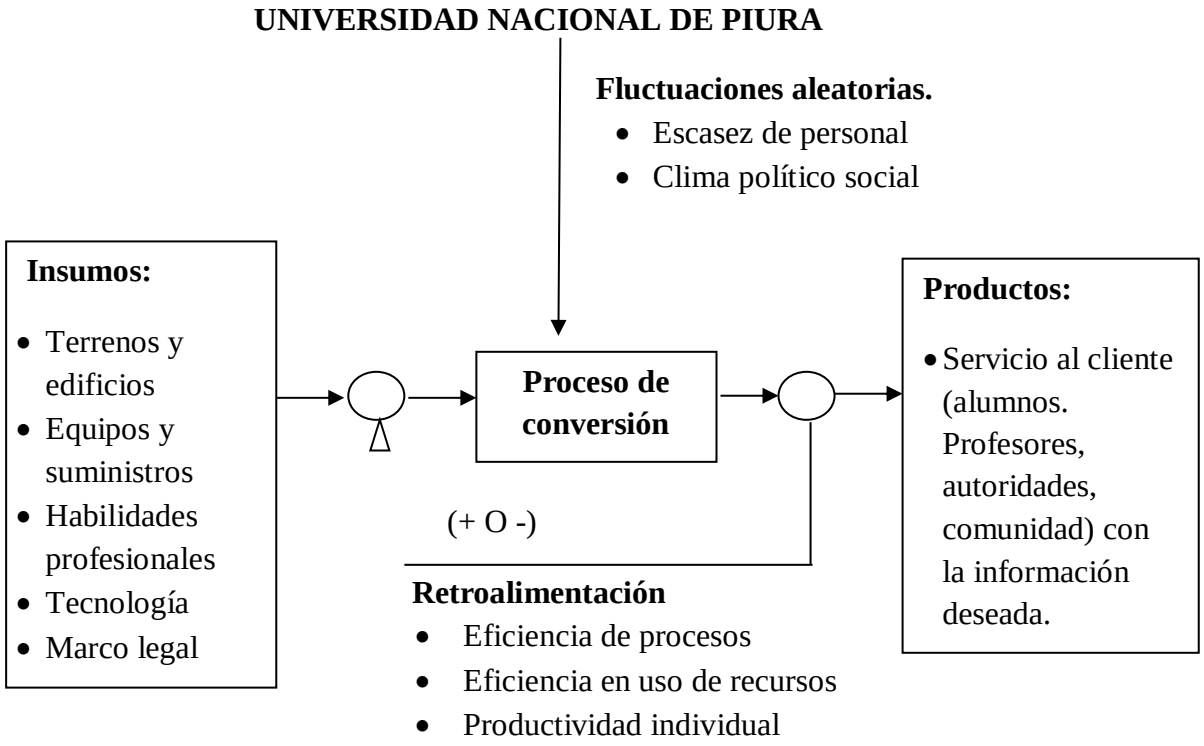

Gráfico 2. 1 Función operacional de la UNP

Fuente:Rosales G. Hugo (2008).

La UNP produce, principalmente, intangibles, sustentados en la formación de profesionales cuyos conocimientos, información y tecnología es del más alto nivel de calidad. Además de la oferta de servicios a la comunidad local y regional.

Para generar estos productos el sistema requiere los siguientes insumos:

- Terrenos y edificios (infraestructura ad hoc para servicios educativos)
- Habilidades profesionales: profesionales capacitados para la generación y transmisión del conocimiento, así como para el desempeño de las funciones administrativas necesarias.
- Equipos y suministros necesarios para la generación de los servicios.
- Marco legal en el que se sustenta la operación para la generación de los servicios: Ley Universitaria, Estatuto, Reglamentos.
- Tecnologías de Información y comunicaciones, sustentado en el conjunto de procesos, procedimientos que permiten la obtención de resultados en el menor tiempo y costo.

2.2.3. Procesos Académicos.

Es un conjuntos de actividades realizadas y coordinadas por las autoridades competentes (Vice Rectorado Académico, OCRA, Facultades, alumnos) orientado a alcanzar y mejorar los objetivos educativos institucionales y los procesos pedagógicos, con el fin de responder a las necesidades educativas locales y regionales. En el caso específico de la Universidad Nacional de Piura, los procesos académicos involucran la investigación, la planificación estratégica del quehacer académico (el planeamiento y la programación académica), producción de materiales didácticos, la articulación, ejecución y evaluación de los procesos de la enseñanza y del aprendizaje" (Reglamento académico, 2006).

De los procesos que tiene la Universidad se ha seleccionado algunos de ellos dentro del ámbito académico y que son importantes y determinantes de su gestión, los cuales mencionó a continuación y están fundamentados en la delimitación de la investigación.

1. Calendarización Académica.
2. Programación Académica por Semestre.
3. Proceso de Modificación de notas.
4. Proceso de Emisión de Actas.
5. Proceso de Inscripción por cursos.
6. Procesos de Desarrollo de Sistemas.
7. Procesos de Soporte Informático.

2.2.4. Sistema Académico

Rosales G. Hugo (2008) en su investigación Mejora de la Eficiencia en el Proceso Académico de Matrícula e Inscripción por cursos en la Universidad Nacional de Piura define al Sistema Académico como un conjunto de procedimientos basados en los reglamentos de la UNP, automatizados mediante el uso de computadoras, para gestionar la información académica. Considerando como información académica, los resultados de los procesos académicos, que, Estatutaria y Reglamentariamente, sintetizan las atribuciones que a continuación se detallan, y que están vinculados a los siguientes actores:

1. Estudiantes: Esta categoría de actores comprende a los estudiantes regulares, especiales y matriculados, graduados, retirados (por rendimiento académico, voluntad propia, abandono).
2. Docentes: Esta categoría de actores comprende a los profesores ordinarios, contratados y jefes de práctica.
3. Administración académica: Comprende a la Oficina Central de Registro y Coordinación Académica, la Oficina Central de Admisión, Secretarías Académicas de Facultades, Directores de Departamento, Directores de Escuela y Decanos. La Oficina de registro realiza las consultas sobre todo los procesos académicos de estudiante y profesores, menos de autoridades, registro y gestión de cursos, emisión y registro de actas, modificación denotas. Las Secretarias Académicas, solo realizan consultas de sus facultades. Los Directores de departamento, Directores y Decanos hacen consultas específicas sobre su facultad.
4. Autoridades: Esta categoría de actores comprende al Rector y al Vicerrector Académico.

2.2.5. Organización Académica.

A) Estructura Académica:

La Universidad Nacional de Piura se organiza y establece su régimen académico por facultades a nivel de pregrado, a nivel de perfeccionamiento por la Escuela de Posgrado. La Escuela de Posgrado y cada Facultad cuenta con la Secretaria Académica como órgano de gestión académica e indispensable para el cumplimiento de los fines y objetivos de la facultad y posgrado respectivamente. La Secretaria Académica está a cargo de un docente ordinario. (Estatuto UNP, 2014).

B) Organización Académica.

La organización académica de la Universidad Nacional de Piura, además de las Facultades y de la Escuela de Posgrado, comprende: Programas Descentralizados, Programas de Formación Continua, Institutos, Escuela Tecnológica Superior, Centros Educativos de Aplicación y otras unidades. (Estatuto UNP, 2014.).

2.2.6. ISO 17799. (ISO 17799, 2000)

El enorme éxito que tuvo el estándar BS 7799 hizo que hoy en día sea aceptado internacionalmente y publicado como ISO 17799. Es importante mencionar que el estándar ISO 17799 no está destinado a ser usado como una normativa de administración de calidad a diferencia del ISO 9000.

Esencialmente el ISO 17799 es un estándar de seguridad, centrado principalmente en requerimientos de control y dividido en diez secciones.

Gráfico 2. 2: Secciones de ISO 17799

Fuente: Leveraging ISO 17799 to Achieve Security Management Best Practices de Evan Tegethoff

A continuación se describe cada sección y las acciones involucradas para asegurar el cumplimiento de sus objetivos:

A. **Políticas de Seguridad:** La administración define en sus políticas de seguridad una dirección estratégica para la seguridad de la información y demuestra su respaldo y compromiso. Una política de seguridad documentada y aplicada es el núcleo vital para la aplicación de un ISMS[1].
B. **Organización de la seguridad:** La organización de la seguridad significa principios y procedimientos para administrar la seguridad de la información. Los principales objetivos de esta sección son:
    - Administrar la seguridad de la información dentro de la organización.
    - Mantener la seguridad de la información de la organización cuando es posible acceder a ella mediante elementos externos, como resultado de algunas facilidades brindadas.
    - Mantener la seguridad de la información de la organización cuando la responsabilidad de su procesamiento se ha encargado a un ente externo.
C. **Clasificación y Control de Activos:** Para proteger activos de información primero se debe elaborar un inventario de todos los activos de información dentro de la organización para así clasificarlos por grado de importancia, y en función a ello asignar acciones de protección a los mismos. Por tanto el principal objetivo de esta sección es:
    - Mantener la apropiada protección de los activos corporativos y asegurar que los activos de información reciban el apropiado nivel de protección.
D. **Seguridad de Personal:** Se intenta reducir los riesgos por errores humanos, robo, fraude o abuso de facilidades. El entrenamiento del personal es vital para el adecuado entendimiento de la seguridad de la información, promoviendo un comportamiento adecuado. Por tanto, los principales objetivos de esta sección son:
    - Asegurar que los usuarios estén alerta de las amenazas de la seguridad de la información.
    - Equipamiento adecuado de los usuarios para respaldar las políticas de seguridad de la organización en el curso de un normal desarrollo de trabajo.
    - Minimizar los daños frente a incidentes de seguridad, fallas, etc., buscando aprender de ellos.
E. **Seguridad Física y Ambiental:** Áreas seguras previenen accesos no autorizados, daños, interferencia en las premisas de negocios. Además protegen de pérdidas de

[1] *Information Security Management System(Sistema de Gestión de Seguridad de la Información)*

activos de información, y finalmente de interrupciones propias del negocio. Por lo tanto el principal objetivo de esta sección es:

- Prevenir el robo de información

F. **Administración computacional y de redes**: Los principales objetivos de esta sección son:

- Asegurar un procesamiento de información seguro.
- Mitigar las fallas de sistema.
- Proteger la integridad del software y la información relacionada al mismo.
- Asegurar la disponibilidad e integridad del procesamiento de información y los servicios de comunicación.
- Proteger la seguridad de información en las redes y su infraestructura
- Prevenir daños a los activos de información y asegurar la continuidad de los procesos de negocio.
- Prevenir la pérdida, modificación y uso indebido de la información que es compartida entre organizaciones.

G. **Control de acceso a los sistemas:** Los principales objetivos de esta sección son:

- Controlar el acceso a la información.
- Prevenir accesos no autorizados a los sistemas de información.
- Asegurar la protección de los servicios de red.
- Prevenir accesos no autorizados a las computadoras.
- Detectar actividades no autorizadas.
- Asegurar la seguridad de información cuando se usa tecnología móvil y demás facilidades de red.

H. **Desarrollo y Mantenimiento de Sistemas:** Los principales objetivos de esta sección son:

- Asegurar que criterios de seguridad se tienen en cuenta al momento del desarrollo de sistemas.
- Prevenir la pérdida, modificación o mal uso de la data de los usuarios en las aplicaciones de sistemas.
- Proteger la confidencialidad, autenticidad e integridad de la información.
- Asegurar que los proyectos de TI y sus actividades relacionadas sean conducidas de manera segura.

I. **Administración de Continuidad de Negocios:** Esta sección señala las acciones correctivas y preventivas que deben tomarse en cuenta para hacer frente a interrupciones que afecten las actividades de negocio y para proteger los procesos críticos de negocio de los efectos, fallas o desastres mayores.

J. **Cumplimiento de requerimientos legales:** Esta sección busca reducir las brechas que pudieran existir en cuanto a obligaciones contractuales y regulatorias. Asimismo se busca cumplir con las políticas y estándares previamente establecidos por el ente regulador.

Gráfico 2. 3: Evolución de la Estructura ISO 27001:2013

Fuente: Presentación Collazos M.

2.2.7. ISO/IEC 27001: Tecnologías de Información, Sistemas de Gestión de seguridad de información. Requerimientos.

La presente norma se toma en cuenta dentro del marco regulatorio porque la seguridad de información es el enfoque del gobierno de TI. Es una norma cuya última versión fue publicada en octubre del 2013. Forma parte de la familia 27000 y cubre todo tipo de organizaciones.

Especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema documentado de Gestión de Seguridad de Información en el contexto de los riesgos de negocio que presenta la organización. Indica los requisitos para la aplicación de controles de seguridad según las necesidades de la organización. (ISO 27001, 2013)

Está diseñada para garantizar la selección de controles de seguridad adecuados y proporcionales para proteger los activos de información y brindar la confianza necesaria para los StakeHolders[2]. (ISO 27001, 2013)

La ISO 27001 no se encarga de definir lo que es riesgo u otros aspectos relacionados, sino definir las actividades que guardan relación con el riesgo y mostrar como alinearlas políticas de gestión de seguridad de información con el contexto de gestión estratégica de riesgos. (Calder y Watkins, 2010).

[2] *"StakeHolder" es usado para indicar cualquier persona que tiene una responsabilidad o una expectativa de las tecnologías de información en una organización.* **(Indagochea A.)**

2.2.8. Norma ISO/IEC 27002: Tecnología de Información, Seguridad de Información. Código de práctica para la Gestión de Seguridad de información.

La presente norma se toma en cuenta dentro del marco regulatorio debido a que está relacionada con la norma ISO 27001, pues esta indica cómo debe de aplicarse. Su fecha de publicación data también de octubre del 2013 y se basa en la anterior norma ISO/IEC 27002:2005. Establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de información en una organización. Los objetivos señalados es el de proporcionar una orientación general sobre las metas comúnmente aceptadas de gestión de seguridad de información. (ISO 27002, 2013).

Contiene las mejores prácticas de objetivos de control y controles en las siguientes áreas de gestión de la información de seguridad (ISO 27002, 2013): Política de seguridad, Organización de la seguridad de información, Seguridad de recursos humanos, Gestión de activos, Control de acceso, Criptografía, Seguridad física y ambiental, Seguridad de las operaciones, Seguridad de comunicaciones, Relaciones con los proveedores, Adquisición de sistemas de información, desarrollo y mantenimiento, Gestión de incidentes de seguridad de información, Gestión de la continuidad de negocio y Cumplimiento.

Los objetivos de control y controles de la norma están destinados a ser implementados para cumplir los requerimientos señalados por la evaluación del riesgo. La norma pretende ser una base común y orientación práctica para la elaboración de estándares organizacionales de seguridad y prácticas eficaces de gestión de la seguridad y para ayudar a construir la confianza en actividades interinstitucionales. (ISO 27002, 2013)

En cuanto a la gestión de activos, la norma indica que en sistemas de información complejos puede ser útil designar grupos de activos, los cuales actúan juntos para proveer una función particular, como “servicios”. En este caso, el propietario del servicio es responsable de la entrega del activo.

La norma ISO/IEC 27002:2013 cuenta con 114 controles, 14 Dominios de Seguridad y 35 Objetivos de control, como se puede apreciar en el Anexo Nº4.

2.2.9. **Norma Técnica Peruana NTP ISO/IEC 27001.** (CNB & INDECOPI, 2008) (ISO 27001, 2013).

Es una norma elaborada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos, publicada en el año 2009 y establecida como de uso obligatorio mediante la Resolución Ministerial N° 129-2012-PCM el año 2012, se encuentra alineada al estándar ISO/IEC 27001 - estándar internacional publicado en el año 2005 que provee un modelo a seguir para el establecimiento y mantenimiento de un SGSI. El objetivo principal de esta norma es establecer los requisitos que se deben cumplir para la implementación del SGSI utilizando un enfoque a procesos, lo cual requiere que se tenga disponible la mayor cantidad de documentación respecto a los mismos.

La norma utiliza la metodología Plan-Do-Check-Act – también llamado ciclo de Deming para definir las fases de vida y mejora continua del SGSI a través de un seguimiento del mismo que asegura el mantenimiento de los controles y los cambios necesarios para poder mitigar los posibles nuevos riesgos que aparezcan luego de la implementación del sistema. La versión correspondiente al año 2013 presenta una nueva estructura según el estándar definido por ISO/IEC para todas las normas referentes a sistemas de gestión, facilitando la integración y trabajo conjunto entre los diferentes estándares de gestión publicados por dicha entidad. Este estándar es de uso crítico en los proyectos de análisis y diseño de SGSI's, dado que establece concretamente los pasos implicados en este proceso.

El diseño del SGSI siguiendo las fases del ciclo de Deming comprende las siguientes etapas:

A. Establecimiento:

Se dan las recomendaciones a seguir para establecer el alcance que tendrá el sistema sobre la organización sobre la que se está trabajando. A continuación se realiza un análisis de identificación de activos de información en conjunto con los riesgos y amenazas a los que se encuentran expuestos, además de realizar la valoración tanto de los activos como de los riesgos asociados y los posibles controles que podrían implementarse para mitigar los mismos.

B. Implementación:

En esta fase se implementan las políticas y planes de mitigación que se requieren para poder tratar el riesgo identificado en el alcance del sistema. Como parte de esta etapa se detallan las acciones específicas que se deben realizar como parte del plan de mitigación.

C. Monitoreo y revisión:

El establecimiento de políticas que rijan los procesos desde el punto de vista de la seguridad de los activos de información que los mismos utilizan, requiere que se establezcan también métricas y procedimientos con los cuales se pueda evaluar su eficiencia y determinar si es necesario realizar algún cambio para mejorar su desempeño, el cual es el objetivo principal de esta etapa.

D. Mantenimiento y mejora continua:

Luego de realizar las evaluaciones de desempeño del SGSI en la etapa anterior, se puede identificar cambios que son necesarios para reajustar el alcance o mejorar su eficacia en el control de riesgos.

Esto, sumado a que el SGSI es una entidad que continua vigente a lo largo del tiempo de vida de la organización, hace que el mantenimiento del mismo sea una tarea crítica como parte de su ciclo de vida.

2.2.10. Gestión del riesgo

Estimación de grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

El riesgo indica lo que puede que podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de causalidad y probabilidad de ocurrencia.

Gráfico 2. 4: Elementos del riesgo

Fuente: ISO/IEC 27001, 2013

A) Identificar los riesgos

- Identificar todos aquellos activos de información que tienen algún valor para la organización que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.
- Identificar las amenazas relevantes asociadas a los activos identificados.
- Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
- Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

B) Análisis del Riesgo

Para analizar el riesgo se debe establecer la probabilidad de ocurrencia del mismo, así como sus consecuencias, esto finalmente orientará a la clasificación del riesgo.

Esta fase depende de la información obtenida en la etapa de identificación. Existen dos aspectos principales que determinarán el análisis de riesgo:

- **Probabilidad:** posibilidad de ocurrencia del riesgo, la cual se puede medir con criterios de frecuencia.
- **Impacto:** consecuencias que pueden ocasionar la materialización del riesgo en la organización.

C) Evaluación del riesgo

La evaluación involucra comparar niveles de riesgo con criterios definidos en el contexto. El objetivo de esta evaluación es la de identificar y evaluar los riesgos, los cuales son calculados por una combinación de valores de activos y niveles de requerimiento de seguridad. Con base en esta comparación, se puede considerar la necesidad de tratamiento; además las decisiones se deben tomar de acuerdo con los requisitos legales, reglamentarios y otros.

La evaluación de riesgos también puede tener como resultado la decisión de no tratar el riesgo de ninguna manera diferente de los controles existentes.

D) Tratamiento del riesgo

El tratamiento del riesgo se define como el conjunto de decisiones tomadas con cada activo de información.

Las decisiones para tratar el riesgo pueden incluir las siguientes opciones:

I. **Evitar el riesgo**: La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión comercial del negocio, se modifican, para así poder evitar la ocurrencia del riesgo.

   Las maneras tradicionales para implementar esta opción son:

   - Dejar de conducir ciertas actividades.

- Desplazar activos de información de un área riesgosa a otra.
- Decidir no procesar cierto tipo de información y no se consigue la protección adecuada
- La decisión por la opción de "evitar el riesgo" debe ser balanceada contra las necesidades financieras y comerciales de la empresa.

II.Aceptar el riesgo cuando no es posible mitigarlo y se debe continuar la actividad que lo originó.

- En muchas ocasiones a la empresa se le presentan circunstancias donde no se pueden encontrar controles ni tampoco es factible diseñarlos o el costo de implantar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.
- Cuando la situación se presenta donde es muy costoso para la empresa mitigar el riesgo a través de los controles o las consecuencias del riesgo son devastadoras para la organización, se deben visualizar las opciones de "transferencia de riesgo" o la de "evitar el riesgo".

III. Reducir el riesgo

Para los riegos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente indefinidos por la empresa. Los controles deben obtenerse del anexo "A" del ISO 270001:2013. Al identificar el nivel de los controles es importante considerar los requerimientos de seguridad relacionados con el riesgo, así como la vulnerabilidad y las amenazas previamente identificadas.

Los controles pueden reducir los riesgos valorados en varias maneras:

- Reduciendo la posibilidad que la vulnerabilidad sea explotada por las amenazas.
- Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionado y recuperándose de ellos.

IV. Transferir el riesgo fuera del apetito de riesgo, el riesgo se comparte con una o varias partes, pueden ser agentes externos.

Gráfico 2. 5: Gestión de Riesgos:
Fuente: ISO/IEC 27001:2013

2.2.11. Controles

Son las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza de que se alcanzarán los objetivos del negocio.

Existen varias formas de establecer controles sobre riesgos organizacionales. La siguiente es:

- Disuasivos: su presencia disuade de la comisión de acciones en contra de alguna política o procedimiento establecido y considerado correcto. Por ejemplo: cámaras de vigilancia.
- Preventivos: detectan problemas antes que ocurran por medio de monitoreo constante. Por ejemplo: políticas de contratación.
- Detectivos: detectan y reportan los problemas suscitados por errores u omisiones, en el momento en que éstos ocurren. Por ejemplo: Uso de antivirus.
- Correctivos: minimizan el impacto de una amenaza ya consumada. Por ejemplo: Planes de contingencia. Propios de cada área administrativa y operativa de las organizaciones.

2.3. GLOSARIO DE TÉRMINOS

Hay algunas definiciones importantes relacionadas al tema de seguridad de información y SGSI, que son útiles para una mejor comprensión de este proyecto.

- **La información:** Es un activo que brinda valor al negocio; por ello, se necesita tener una adecuada protección frente a la constante exposición a distintas amenazas y vulnerabilidades. Esta puede adoptar distintas formas, de ahí surge la importancia de conocerlas para poder protegerla adecuadamente, estas formas son: Impresa o escrita en papel Almacenada electrónicamente, Transmitida vía correo o e-mail Mostrada en videos, Hablada en conversaciones
- **Seguridad de Información:** Es la protección de la confidencialidad, integridad y disponibilidad de la información; es decir, es asegurarse que esta sea accesible solo a las personas autorizadas, sea exacta sin modificaciones no deseadas y que sea accesible a los usuarios cuando lo requieran
- **Oficial de Seguridad de Información**: El oficial de seguridad de la información, conocido como CISO por sus siglas en inglés (Chief Information Security Officer), es la persona encargada de planificar, presupuestar y verificar el rendimiento de los componentes de la seguridad de la información. Así como de realizar una correcta gestión de riesgo para la toma de decisiones. Las responsabilidades de cada oficial varían dependiendo de la organización en la que se encuentren, debido a la cultura organizacional que puede existir.
- **Activos de Información** Los activos son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad, necesarios para que la organización funcione y alcance los objetivos que propone su dirección "… algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger".
- **Amenazas:** En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza es todo aquello, ya sea físico o lógico que puede causar un incidente no deseado, generando daños materiales o inmateriales a la organización y a sus activos, como la perdida de información, o de su privacidad, o bien un fallo en los equipos físicos.
- **Sistema de Gestión**: Un sistema de gestión es una estructura probada para la gestión y mejora continua de políticas, procedimientos y procesos de una organización.

  La implementación de un sistema de gestión ayuda a mejorar la efectividad operativa, optimizar costos, lograr mejoras continuas, aumentar la satisfacción de las partes interesadas al negocio y renovar constantemente las estrategias de la organización.
- **Sistema de Gestión de Seguridad de Información**: Conocido como SGSI o ISMS por sus siglas en inglés (Information System Management System) es un sistema de gestión para

establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información, de esta manera un SGSI lo que busca es poder mantener la confidencialidad, integridad y disponibilidad de la información mientras minimiza los riesgos de seguridad de la información.

- **Riesgo:** Un riesgo es cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad.
- **Administrar Riesgos:** Es el uso de la información para estimar el impacto de los riesgos e identificar sus causas, de esta manera se pueden tomar medidas anticipadas ante un incidente.
- **Evaluación del riesgo**: Proceso general de análisis y evaluación del riesgo.
- **Control:** El control es un proceso por el cual la administración verifica si lo que ocurre concuerda con lo que supuestamente debe ocurrir. Permite que se realicen los ajustes o correcciones necesarias en caso se detecten eventos que escapan a la naturaleza del proceso. Es una etapa primordial en la administración, pues, por más que una empresa cuente con magníficos planes, una estructura organizacional adecuada y una dirección eficiente, no se podrá verificar la situación real de la organización si no existe un mecanismo que verifique e informe si los hechos van de acuerdo con los objetivos.
- **Controles:** Los controles son medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales. Una de las clasificaciones más generalizadas es:
  - Preventivos: Reducen las vulnerabilidades.
  - Detectivos: Descubren amenazas o escenarios previos a ellas permitiendo activar otros controles.
  - Correctivos: Contrarrestan el impacto de la ocurrencia de una amenaza.
  - Disuasivos: Reducen la probabilidad de ocurrencia de las amenazas.

    En el NTP ISO/IEC 17799 también se utiliza el control como un sinónimo de contramedida.
- **Seguridad de Información:** Es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. Se logra implementando un adecuado conjunto de controles incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.
- **Evento de seguridad de información**: Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de seguridad de información

o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad.

- **Política:** Dirección general y formal expresada por la gerencia
- Vulnerabilidad: Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.
- **Confidencialidad**: Protección de la información confidencial del acceso o divulgación por parte de entidades – personas jurídicas o naturales – no autorizadas al mismo, tanto por parte del originario de la información como por parte de la entidad que maneja la misma.
- **Integridad:** Protección de la información frente a la modificación o eliminación sin la autorización o accesos necesarios. De esta forma se garantiza que la información sea la correcta en todo momento.
- **Disponibilidad**: La información se encuentra accesible en todo momento, bajo demanda de todo usuario que se encuentre autorizado a poder acceder a la misma.
- **Autenticación**: Mediante esta propiedad, se permite identificar a la persona o personas que han generado la información que se está verificando, permite una validación en la autoría de la información por parte de un usuario específico.

CAPÍTULO III: MARCO METODOLÓGICO

3.1. ENFOQUE Y DISEÑO

Se realizó una investigación Aplicada debido a que se ha recolectado información cuantitativa y cualitativa, la investigación fue metodológicamente de tipo no experimental.

3.2. SUJETOS DE LA INVESTIGACIÓN

3.2.1. Población

En la población los objetos de estudios han sido el universo de Procesos que desarrolla la Organización Académica de la Universidad Nacional de Piura:

En estos procesos críticos[3] se centra el flujo de información necesaria para el éxito de la institución (Reglamento Académico de la UNP, 2006)

3.2.2. Muestra.

Se tomó los procesos académicos más relevantes y que tienen deficiencias dentro del universo correspondiente.

- Calendarización Académica.
- Programación Académica por Semestre.
- Proceso de Inscripción por cursos.
- Proceso de Modificación de notas.
- Proceso de Emisión de Actas.
- Procesos de Desarrollo de Sistemas.
- Procesos de Soporte Informático

3.3. MÉTODOS Y PROCEDIMIENTOS.

Las reuniones iniciales llevadas a cabo con el personal de la Universidad Nacional de Piura Centro de Informática y Telecomunicaciones (CIT) y Docentes de la facultad de Ingeniería Industrial permitieron confirmar el alcance del trabajo. Se identificó las áreas que participaron en el desarrollo de cuestionarios , programándose las entrevistas, tanto a personal estratégico como a personal operativo.

Éstos métodos y procedimientos dieron lugar a la realización de un análisis de brechas cuyo resultado de la calificación permitió determinar el nivel de cumplimiento general de la institución, y por dominios. A partir de esta calificación, y de acuerdo al análisis de los

[3] *Crítica: Desde una perspectiva de objetivos son aquellos que influyen directamente en el éxito del negocio.*

documentos, entrevistas, modelamiento de procesos académicos, valorización de activos y plan de tratamientos de riesgos se identificaron los controles requeridos para reducir las brechas respecto a la gestión de seguridad de información.; favoreciendo en la toma de decisiones para la propuesta del Diseño del Sistema de Gestión de Seguridad de la Información.

Para el análisis de datos se utilizó como herramienta a Microsoft Excel, para lo cual se procedió inicialmente a ingresar las respuestas a cada pregunta incluida en cada dominio. Se definió un modelo donde se ingresaron la cantidad de preguntas por dominio y objetivo de control para cada pregunta con las respuestas de los encuestados. Se definen tablas para cada dominio, se encuentra la frecuencia por pregunta de acuerdo a las alternativas u opciones proporcionadas, para ello se procedió a utilizar la función estadística CONTAR.SI (……), para encontrar el número de presencias que hay por pregunta, esta frecuencia también se determina en forma porcentual. El análisis de la investigación se puede apreciar en el Anexo Nº 1.

Se diseñó una tabla resumen que cuenta con los dominios y su nivel de cumplimento de la seguridad de la información en la institución. Asimismo se crearon los gráficos de barras de la información obtenida en esta etapa de evaluación. Los resultados del análisis se encuentran detallados en el Capítulo IV, sección 4.2.

3.4. TÉCNICAS E INSTRUMENTOS

La recopilación de información se basa en la revisión de información y documentación, entrevistas a técnicos del área académica, entrevistas a personal usuario, inspección de las áreas de información y la evaluación de las respuestas de los cuestionarios. Todas estas fuentes de información son consideradas para poder determinar la calificación de los niveles de cumplimiento sobre aspectos de seguridad de información.

Se consideró dos tipos distintos de cuestionarios:

- Cuestionarios dirigidos a Jefe del área de Tecnología de Información
- Cuestionario dirigido a personal usuario.

Los cuestionarios permitieron, como una referencia central, medir el nivel de cumplimiento de los dominios de la gestión de la seguridad de la información. Los dominios considerados son los siguientes:

1. Política de Seguridad.
2. Organización de la seguridad de la información.
3. Seguridad Ligada a los Recursos Humanos

4. Gestión de Activos.
5. Control de Accesos.
6. Seguridad en la Operativa
7. Seguridad en las Telecomunicaciones.

Antes que los usuarios inicien con el desarrollo de los cuestionarios, se determinó el nivel de objetividad de las respuestas, la forma como estos cuestionarios deben ser desarrollados, y el sustento que cada una de las respuestas debe tener. La explicación, sobre estos aspectos, se efectuó a través de reuniones con el personal encargado de resolver los cuestionarios.

3.5. ASPECTOS ÉTICOS

En el desarrollo de la investigación, se realizó un trato adecuado al personal, docentes, alumnos y el ambiente procurando su bienestar. Asimismo, se respetaran los derechos de autor y la originalidad de la investigación.

CAPÍTULO IV: RESULTADOS Y DISCUSIÓN

4.1. ANÁLISIS DE BRECHAS

4.1.1. Desarrollo de Entrevistas al personal UNP.

Las entrevistas realizadas son unas de las principales fuentes de información necesarias para le realización del presente estudio. Algunas de ellas se efectuaron para recoger información sobre los esquemas de seguridad actualmente implementados. Otras se orientaron a identificar las debilidades actuales del sistema informático (entrevistas efectuadas personal del CIT y docentes de la Facultad de Industrial).

Éstas permitieron obtener la visión con respecto a los conceptos de gestión de seguridad de la información. De la misma forma se mantuvo entrevistas con el personal operativo, para verificar la forma como actualmente se identifican los controles de seguridad de información y observar la manera como se evalúa el cumplimiento de dichos controles.

Las entrevistas con personal operativo fueron enfocadas a identificar errores e incongruencias de los sistemas de información. En estas visitas realizadas también se abordó temas concernientes al servicio que brinda el Área Académica y los esquemas actuales de seguridad y respaldo de información. Asimismo se recopiló información de los procesos académicos y los riesgos que conlleva en la actualidad. Finalmente, se entregó el inventario de activos de información solicitado para realizar y continuar con la presente investigación.

4.1.2 Revisión de los documentos referidos a la Seguridad de Información.

Se solicitaron un conjunto de documentos para corroborar la existencia o falta de políticas y controles de seguridad de la información, obtuviendo la respuesta que existen políticas y controles minimos implementados pero no están documentados. La inexistencia de estos documentos no necesariamente implica la no aplicación de éstos en la institución. Una forma de saberlo es a través del resultado de los cuestionarios y a través de las entrevistas realizadas a los usuarios, mediante las cuales se pudo inferir el bajo nivel de difusión, de conocimiento y la aplicación de estos estándares de seguridad de información. Se obtuvo directivas sobre el uso del Antivirus, las cuales se puede apreciar en el Anexo Nº 5. Para la presente investigación se mencionan algunas políticas y directivas que la institución ha implementado para el desarrollo de sus procesos académicos:

- Política del uso de un Antivirus.
- Politica del uso del Internet.

- Política del uso del correo corporativo.
- Política de Protección a la Red a cargo de la EmpresaTelefónica.
- Politica de Acceso al Data Center.
- Política de acceso a los sistemas de información, servidores y estaciones de trabajo.
- Política de Resticción a la instalación de aplicaciones en el servidor de aplicaciones.
- Politica de respaldo de información semestralmeste por parte del usuario.
- Política de cambio de contraseña cada 30 días.
- Directiva del uso y asignación de los equipos.
- Directiva sobre las el uso y funciones de los sistemas de información por parte de los trabajadores.
- Directiva para restricción al acceso a las redes sociales, descarga de programas y bloqueo de algunas páginas de internet.

4.1.3. Desarrollo de las observaciones de campo

Para constatar la seguridad física se realizó una inspección para verificar la existencia de perímetros de seguridad, el estado de la estructura física respecto a equipos informáticos, ambientes, el acceso a las instalaciones, conexiones entre equipos, distribución de estos equipos, estabilizadores, etc. que favorezca a la investigación. Se revisó los ambientes de cómputo y de comunicaciones tanto del local de la oficina principal, como el DataCenter. También se verificó el lugar donde se guarda el respaldo de información (backups) es el mismo DataCenter en un Servidor de Backups. Asimismo, se observó los de acceso físico a los ambientes donde se guarda información sensible (archivo de expedientes). También se verificó la existencia de controles físicos para mitigar riesgos, como sensores de humo, cámaras de vídeo, extintores, respaldo eléctrico, entre otros. En el DataCenter se comprobó que no existen cámaras de video.

4.1.4. Desarrollo de los cuestionarios

Se implementó cuestionarios divididos en los dominios del ISO/IEC 27001, de los cuales se eligieron 7 y sus objetivos de control que abarcan los diferentes aspectos de seguridad.

Se apersonó al personal tanto en el Área de Desarrollo, Redes, Soporte Informático del Centro de Informática y Telecomunucaciones y docentes de la Facultad de Industrial, entregándoles un cuestionario, indicando que tenían un tiempo prudencial para resolverlo, debido por la cantidad de preguntas que tenían que resolver.

Este procedimiento se realizó reiteradas veces debido a que el personal se le presentaba diligencias improvistas o sobrecarga laboral. Los cuestionarios se pueden apreciar en el Anexo Nº2.

4.2. SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN DE LOS PROCESOS ACADÉMICOS .

La seguridad de información es un tema que no sólo compete al área de informática, sino que involucra a todas y cada una de las áreas de la institución, empezando por la Alta Dirección (Rector y Vice Rectorado Académico), que debe participar activamente en el proceso de implementación de la gestión de seguridad de información, fortaleciendo, de esta forma, el proceso de concientización.

Aquí se muestran los resultados de las brechas identificadas y los controles de seguridad de información, según estándar ISO/IEC 27001, los cuales permitirán reducir estas brechas. El primer resultado que se muestra es el porcentaje de cumplimiento global, es decir la totalidad de los controles considerados en el presente estudio, que son 49 controles específicos. Luego se muestra el cumplimiento por dominios. Para cada uno de los dominios el nivel máximo de cumplimiento es el 100% según la norma ISO/IEC 27001. Los controles se pueden evidenciar en el Anexo Nº4.

Actualmente la Universidad Nacional carece de un Sistema de Gestión de la Seguridad de la Información establecido y documentado. Sin embargo por criterio propio y por las exigencias demandas de los objetivos institucionales entre otros,se ha implementado políticas y controles básicos para proteger y mitigar los riesgos de la información y activos en el desarrollo de sus procesos académicos.

Por lo tanto, de acuerdo al análisis de brechas efectuado en el presente estudio, la situación actuald de Seguridad de la Información en los Procesos Académicos logra un nivel de cumplimiento global del 39%. (Gráfico 4.1). Para lo cual la NTP ISO/IEC 27001, determina que deben cumplirse todas las acciones de control que propone para minimizar los riesgos que puedan aparecer, También se ha encontrado que la mayor parte de dominios no cumplen con los objetivos de control requeridos, generando una incidencia negativa en las acciones de control que se deberían tener en cuenta al momento de salvaguardar los activos de la institución. (Gráfico 4.2)

CUMPLIMIENTO GLOBAL SEGURIDAD DE LA INFORMACIÓN DE LOS PROCESOS ACADÉMICOS

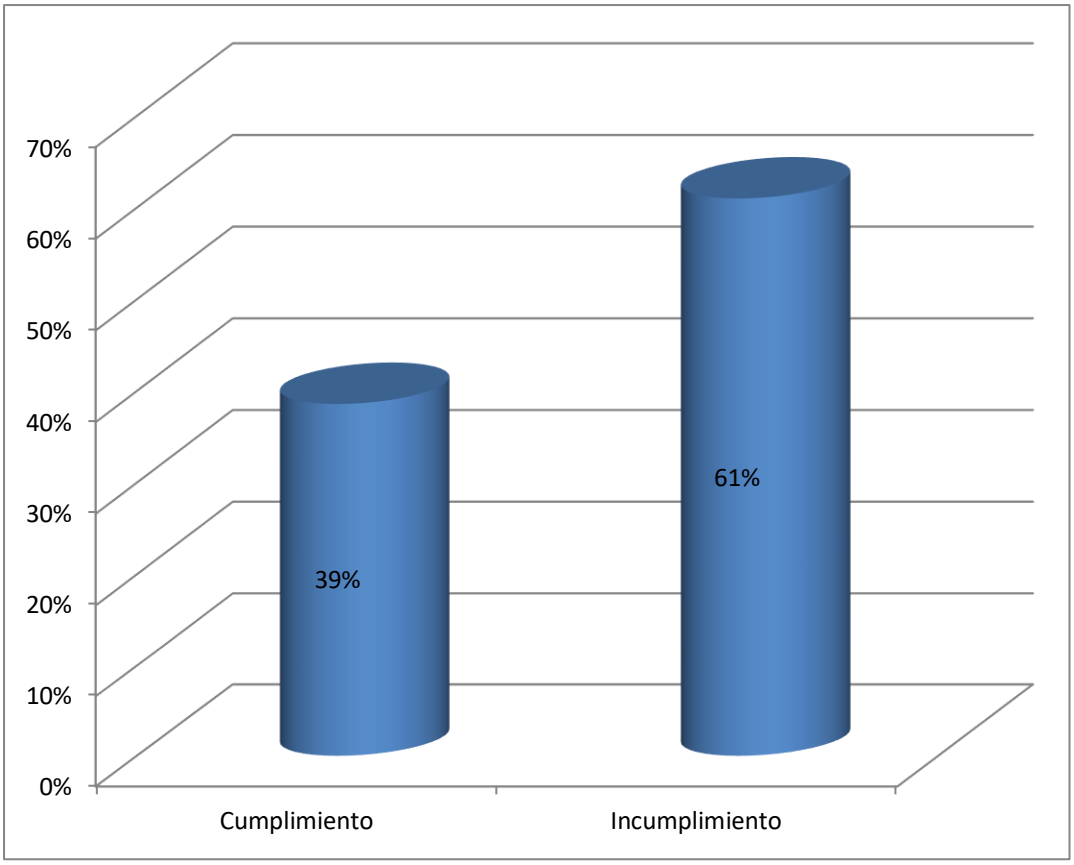

Gráfico 4. 1 Cumplimiento Global de la Seguridad de la Información de los Procesos Académicos de la UNP.

Elaboración propia.

El presente Análisis ha determinado que la Seguridad de la Información de los Procesos Académicos en la Universidad Nacional de Piura, con respecto al estándar ISO/IEC 27001, cumple con un 39%, debido a la escasa implementación de controles y políticas seguridad de información documentadas y difundidas en toda la institución.

4.3. CUMPLIMIENTO POR DOMINIOS.

A continuación se grafica el cumplimiento por dominios. Tal como se puede apreciar en el gráfico 4.2, de acuerdo a la situación actual, los dominios de POLÍTICAS DE SEGURIDAD,ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD LIGADA A LOS RECURSOS HUMANOS, son los que tienen un menor porcentaje de cumplimiento. Para un mayor detalle, en el Anexo Nº 2 se encuentra el análisis completo.

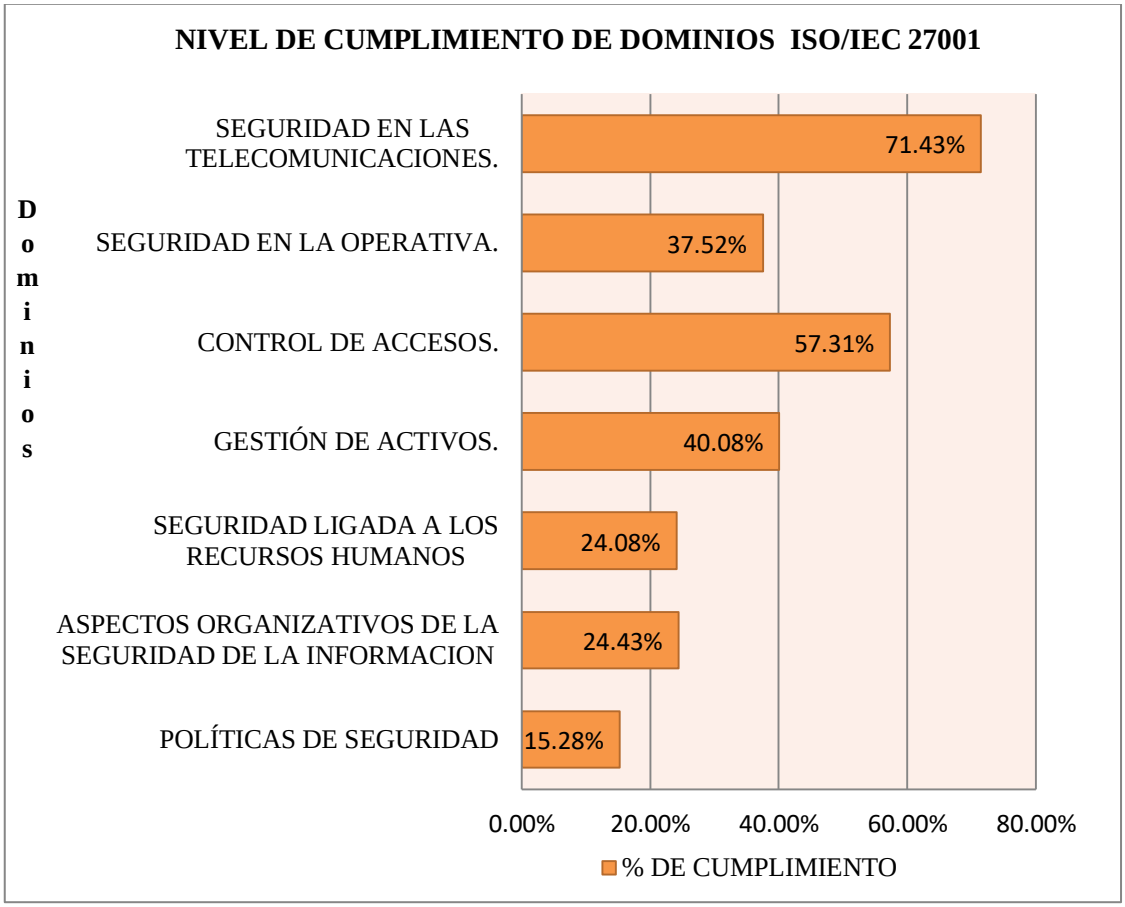

Gráfico 4. 2: Cumplimento por Dominios de Seguridad de Información de los Procesos Académicos de la UNP

Elaboración propia

.

Tabla 4. 1: Cumplimiento por Dominio de Seguridad de la Información delos Procesos Académicos de la UNP

DOMINIOS ISO/IEC 27001	PORCENTAJE DE CUMPLIMIENTO
POLÍTICAS DE SEGURIDAD	**15.28%**
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	**24.43%**
SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**24.08%**
GESTIÓN DE ACTIVOS.	**40.08%**
CONTROL DE ACCESOS.	**57.31%**
SEGURIDAD EN LA OPERATIVA	**37.52%**
SEGURIDAD EN LAS TELECOMUNICACIONES.	**71.43%**

4.3.1. Dominio Política de Seguridad

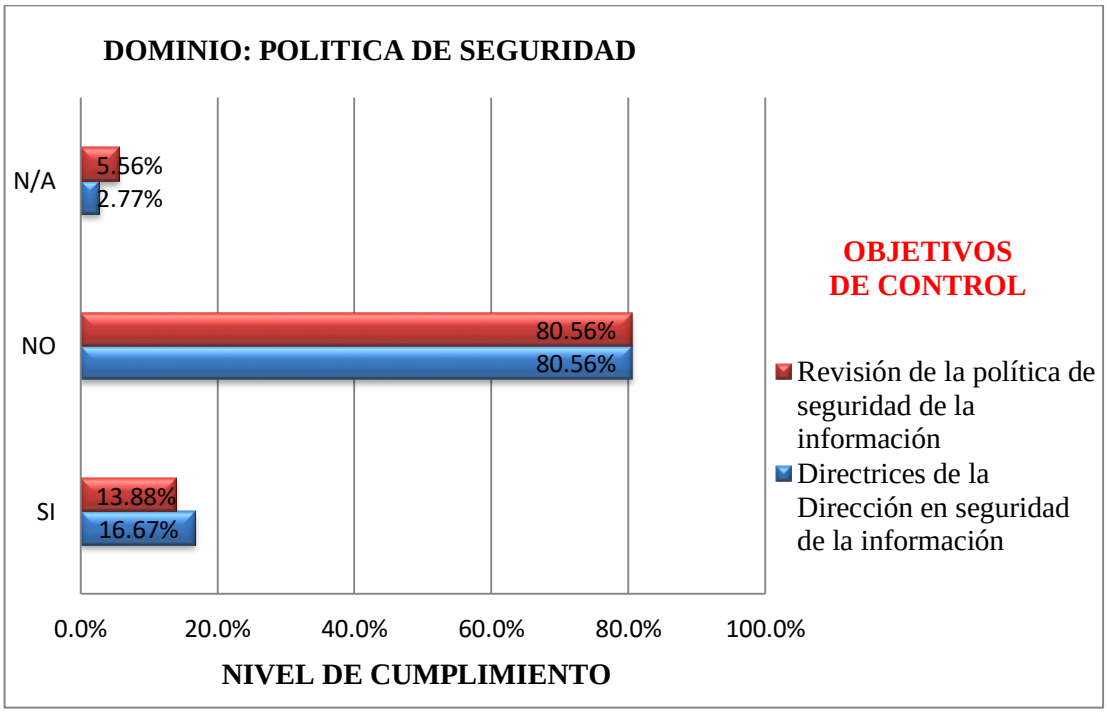

Gráfico 4. 3: Dominio Política de Seguridad

Elaboración propia

Una Política de Seguridad es importante porque establece directrices fundamentales que regirán todas las acciones relacionadas con la Seguridad de la Información dentro de una organización.

Teniendo en cuenta que la norma ISO /IEC 27001, determina que deben cumplirse todas las acciones de control para minimizar los riesgos que pueda sufrir. Sin embargo se ha encontrado un bajo porcentaje de cumplimiento en los objetivos de control de este dominio según el análisis realizado a la Universidad Nacional de Piura, como se puede apreciar en el gráfico 4.3.

La institución no está cumpliendo con los control necesarios que exige la norma poniendo en riesgo los objetivos institucionales que garantizan confiabilidad, integridad, disponibilidad y auditabilidad de la información. Ante ello se presenta a continuación en la tabla 4.2, un resumen de los objetivos de control del dominio para saber su cumplimiento

Tabla 4. 2: Resumen de los Objetivos de Control Política de Seguridad

Objetivos de Control	Porcentaje de incumplimiento	Porcentaje de cumplimiento	N/A
Directrices de la Dirección en seguridad de la información	80.56%	16.67%	2.77%
Revisión de la política de seguridad de la información	80.56%	13.88%	5.56%

Como se aprecia en la tabla 4.2, se ha encontrado que más del 50% incumple con la implementación y documentación de políticas y controles que la norma propone. Además el bajo porcentaje de cumplimiento, es debido a que la institución cuenta con políticas y controles mínimos y básicos para sus actividades académicas.

El alto porcentaje de incumplimiento, es debido a que no existe una existe una política general de seguridad de la información documentada en la institución, no se ha publicado la política de seguridad en la institución y tampoco tienen conocimiento de los procedimientos de la Política de seguridad cuando ocurre un evento de seguridad. Estos son los valores más bajos de las preguntas realizadas.

Por lo tanto se concluye que el riesgo del domino es alto debido a que existe un bajo porcentaje de cumplimento, que es del 15.28%, según la tabla 4.1: Cumplimiento de los dominios.

4.3.2. Dominio: Aspectos Organizativos de la Política de la Seguridad de la Información.

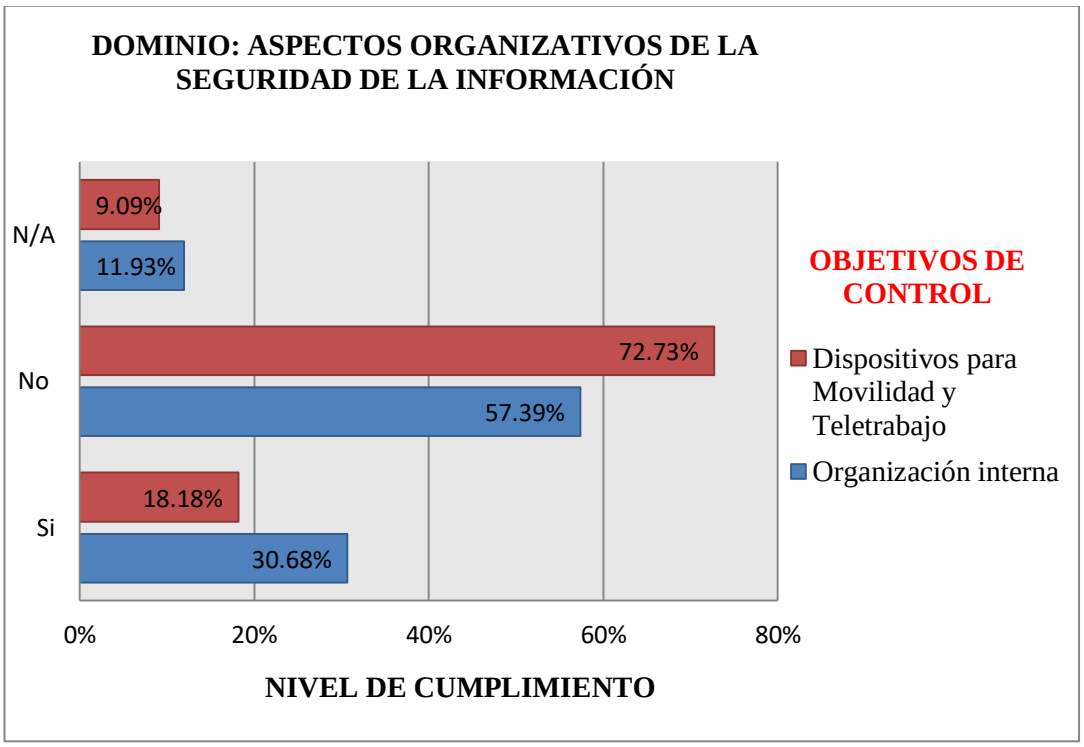

Gráfico 4. 4: Dominio Aspectos Organizativos de la Política de la Seguridad de la Información

Elaboración propia

El objetivo del presente dominio es establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la organización.

Según la norma ISO /IEC 27001, determina que deben cumplirse todas las acciones de control para minimizar los riesgos que pueda sufrir. Sin embargo según el análisis realizado, la Universidad Nacional de Piura no está aplicando los controles necesarios que exige la norma como se aprecia en el gráfico 4.4. Ante ello, se presenta una tabla resumen de los objetivos de control del dominio para saber su cumplimiento.

Tabla 4. 3: Resumen de los Objetivos de Control del Dominio Aspectos Organizativos de la Política de Seguridad.

Objetivos de Control	Porcentaje de incumplimiento	Porcentaje de cumplimiento	N/A
Organización Interna	57.39%	30.68%	11.93%
Dispositivos para movilidad de Teletrabajo	72.73%	18.18%	9.09%

Como se puede apreciar en la tabla 4.3, se ha encontrado que más del 50% del dominio no cumple con los controles requeridos por la norma. El alto porcentaje de incumplimiento se debe a que, no existe un oficial de seguridad de la información en la institución,no existe un comité de Seguridad de la información formado por las áreas de la institución, una política formal y medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones, políticas claramente definidas para la protección, no sólo de los propios equipos informáticos, sino, en mayor medida, de la información almacenada en ellos, no existe políticas y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo y finalmente no existe un programa de capacitación permanente para desarrollar habilidades y competencias para la seguridad de la información al personal encargado de los sistemas de información y el personal que la labora no tiene asignada roles o responsabilidades sobre la seguridad de la información.

Por lo tanto, se concluye que el Dominio no cumple con todos los objetivos de control que propone la norma, debido a la escasa implementación de controles, poniendo en riesgo la seguridad de la información.

El bajo porcentaje de cumplimiento del Dominio es del 24.43%, según la tabla 4.1: Cumplimiento de los dominios.

4.3.3. Dominio: Seguridad Ligada a los Recursos Humanos.

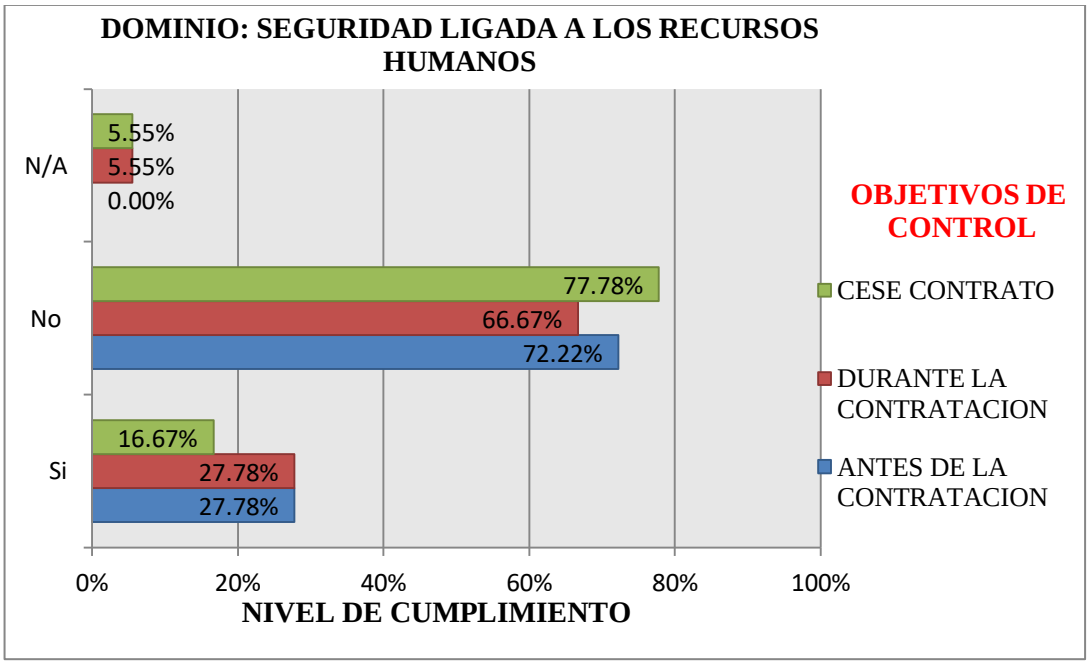

Gráfico 4. 5: Dominio Seguridad de Recursos Humanos

Elaboración propia

El objetivo del presente dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

Según la norma ISO/IEC 27001, determina que deben cumplirse todas las acciones de control para minimizar los riesgos que pueda sufrir. Sin embargo como apreciamos en el gráfico 4.5 y de acuerdo al análisis realizado, la Universidad Nacional de Piura no ha cumplido con todos los controles que la norma exige. Ante ello, se presenta a continuación la siguiente tabla resumen de los objetivos de control para conocer el cumplimiento del dominio:

Tabla 4. 4: Resumen de los Objetivos de control del Dominio: Seguridad Ligada a los Recursos Humanos

Objetivo de Control	Porcentaje de incumplimiento	Porcentaje de cumplimiento	N/A
Antes de la contratación	72.22%	27.78%	0.00%
Durante la contratación	66.67%	27.78%	5.55%
Cese de contrato	77.78%	16.67%	5.55%

Como se puede apreciar en la tabla 4.4, se ha encontrado que más del 50% de los Objetivos de control del Domnio incumplen con la implementación de los controles, mientras que existe un bajo porcentaje de cumplimiento, esto debido a que no se ha firmado un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad, ni se ha proporcionado un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad.

Por lo tanto se concluye que, el domino **SEGURIDAD LIGADA A LOS RECURSOS HUMANOS,** no cumple con todos los objetivos de control que propone la norma, poniendo en riesgo la seguridad de la información por el bajo porcentaje de cumplimiento, que es del 24.08%, según la tabla 4.1: Cumplimiento de los dominios.

4.3.4. Dominio Gestión de Activos.

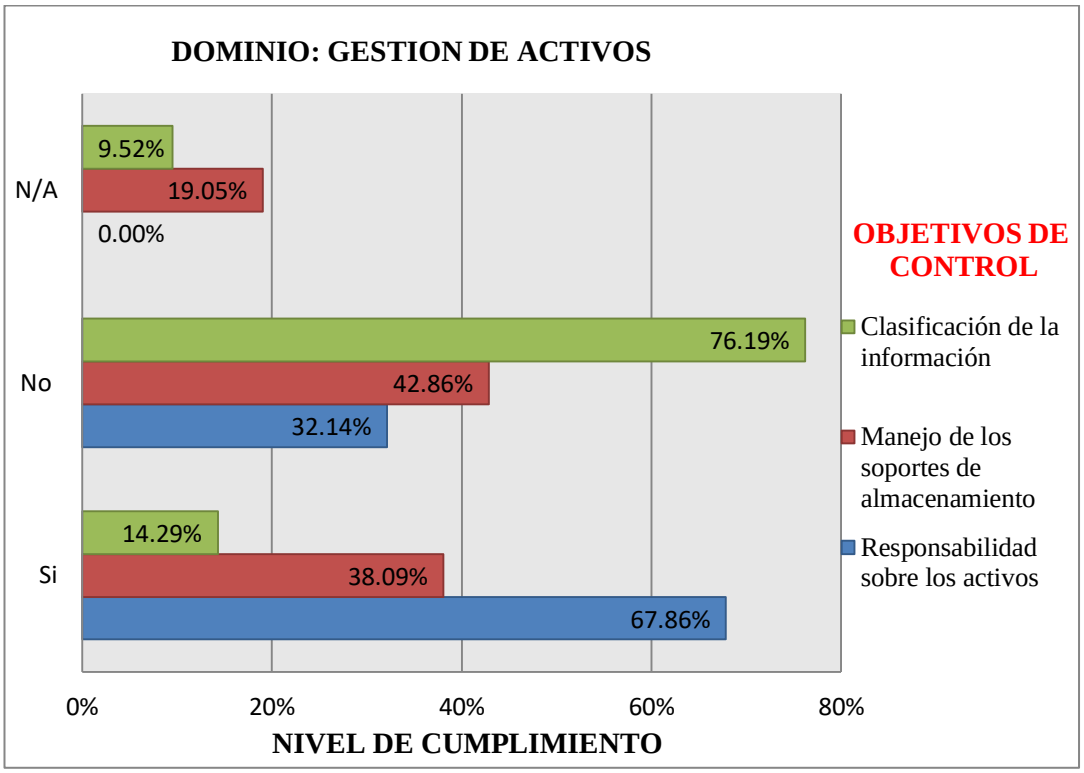

Gráfico 4. 6: Dominio Gestión de Activos

Elaboración propia

El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.

Según la norma ISO /IEC 27001, determina que deben cumplirse todas las acciones de control para minimizar los riesgos que pueda sufrir. Sin embargo según el análisis realizado, la Universidad Nacional de Piura no está aplicando los controles necesarios que exige la norma como se aprecia en el gráfico 4.6. Ante ello, se hace un resumen de los objetivos de control para saber el cumplimiento del dominio en la siguiente tabla:

Tabla 4. 5: Resumen de los Objetivos de control Gestión de Activos

Objetivo de control	Porcentaje de incumplimiento	Porcentaje de cumplimiento	N/A
Responsabilidad sobre los activos	32.14%	67.86%	0.00%
Manejo de los soportes de almacenamiento	42.86%	38.09%	19.05%
Clasificación de la información	76.19%	14.29%	9.52%

Como se puede apreciar en la tabla 4.5, se ha encontrado un bajo porcentaje de incumplimiento con la excepción del objetivo de control Clasificación de la información que es del 76.19%. Cabe indicar que el porcentaje de cumplimiento también es bajo con la excepción del Objetivo de Control Responsabilidad sobre los activos que es del 67.86%, pero en cambio hay un condiserable porcentaje de desconocimiento de la gestión de activos que llega hasta el 19.05%. Esto es debido a que la mayor parte de la institución no usa códigos de barras para facilitar las tareas de realización de inventario y para vincular equipos de TI que entran y salen de las instalaciones con empleados, escasa información documentada sobre el uso adecuado de los activos y tratamiento de información, y no posee de bitácoras de fallas detectadas en los equipos, entre otras.

Por lo tanto se concluye que el dominio: **Gestión de Activos** no cumple con todos los objetivos de control que propone la norma ISO/IEC 27001, poniendo en riesgo la seguridad de la información por el bajo porcentaje de cumplimiento, que es del 40.08%, según la tabla 4.1: Cumplimiento de los dominios.

4.3.5. Dominio Control de Acceso

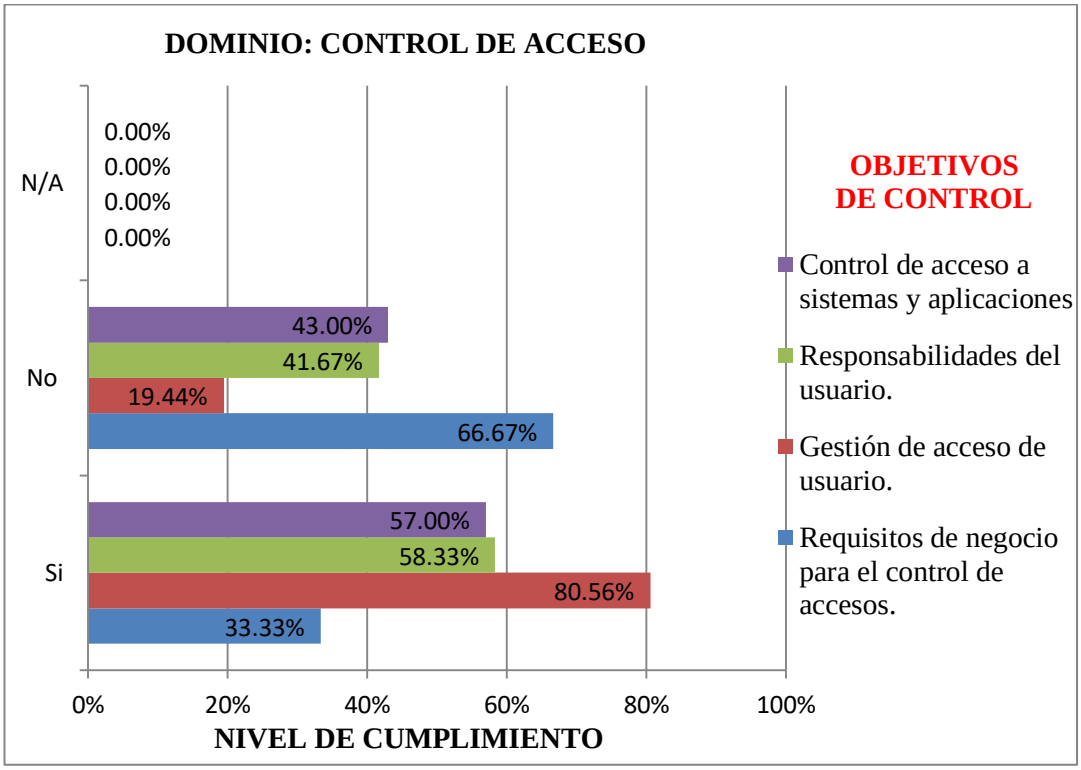

Gráfico 4. 7: Dominio Control de Acceso

Elaboración propia

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

Según la norma ISO/IEC 27001, determina que deben cumplirse todas las acciones de control para minimizar los riesgos que pueda sufrir, sin embargo de acuerdo al análisis realizado, se ha encontrado que la Universidad Nacional de Piura no cumple con todos los controles que la norma exige, como se puede apreciar en el gráfico 4.7.Teniendo en cuenta esto, se ha detallado en la tabla 4.6, el resumen de los objetivos de control para conocer el cumplimento del dominio:

Tabla 4. 6: Resumen de los Objetivos de Control del Dominio Control de Acceso

Objetivo de Control	Porcentaje de incumplimiento	Porcentaje de cumplimiento	N/A
Requisitos de negocio para el control de accesos	66.67%	33.33%	0.00%
Gestión de acceso de usuario	19.44%	80.56% s	0.00%
Responsabilidades del usuario	41.67%	58.33%	0.00%
Control de acceso a sistemas y aplicaciones	43.00%	57.00%	0.00%

Como se puede apreciar en la tabla 4.6, se ha encontrado un porcentaje de incumplimiento de los objetivos de control menor del 50% excepto el Objetivo de Control Requisitos de negocio para el control de acceso, que representa el 66.67% mientras que existe un mayor porcentaje de cumplimiento. En este dominio es favorable el cumplimiento en cuanto se ha aplicado más del 50% de los controles que la norma propone, sin embargo no es suficiente ya que se exige cumplir con todos los controles para mitigar los riesgos que se presentan. Esto es debido a que , no existe una política de control de acceso documentada, no existen controles documentados para el acceso a los recursos, no se ha definido y documentado claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo, no se controla y restringe el uso de utilidades de software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas y los practicantes pre y profesionales no cuentan con funciones y responsabilidades específicas.

Por lo tanto se concluye que el dominio no cumple con todos los objetivos de control propuestos por la norma, generando amenazas que ponen en riesgo la seguridad de la

información. El porcentaje de cumplimiento es del 57.31%, según la tabla 4.1: Cumplimiento de los dominios.

4.3.6. Dominio: Seguridad en la Operativa.

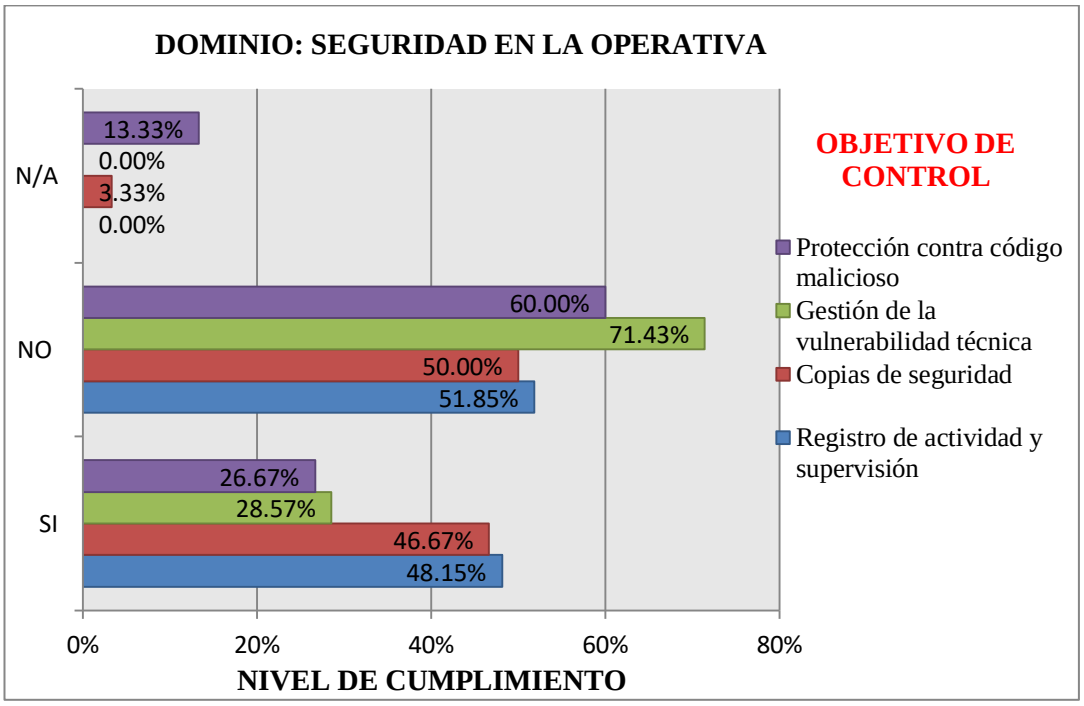

Gráfico 4. 8. Dominio Seguridad en la Operativa

Elaboración propia

El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

Según la norma ISO/IEC 27001, determina que deben cumplirse todas las acciones de control para minimizar los riesgos que pueda sufrir, pero se ha encontrado de acuerdo al análisis realizado, que la Universidad Nacional de Piura no cumple con todos los controles que exige la norma técnica. Ante ello se muestra un resumen de los resultados en la siguiente tabla:

Tabla 4. 7: Resumen de los objetivos de control del Dominio Seguridad en la Operativa

Objetivo de Control	Porcentaje de incumplimiento	Porcentaje de cumplimiento	N/A
Registro de actividad y supervisión	51.85%	48.15%	0.00%
Copias de seguridad	50.00%	46.67%	3.33%
Gestión de la vulnerabilidad técnica	71.43%	28.57%	0.00%
Protección contra código malicioso	60.00%	26.67%	13.33%

Como se puede apreciar en la tabla 4.7, existe un porcentaje mayor del 50% de incumplimiento y un porcentaje bajo de cumplimiento de los objetivos de control, debido a que no existe controles documentados sobre el acceso físico a las copias de seguridad, no se almacenan las copias de seguridad en un lugar de acceso restringido, los dispositivos que tienen las copias de seguridad, no son almacenados fuera del edificio de la institución, las copias de seguridad no son encriptados, no existe un programa de mantenimiento preventivo para el dispositivo del SGBD, no se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio y finalmente no se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado.

Por lo tanto se concluye que el dominio, no cumple con todos los objetivos de control propuestos por la norma, poniendo en riesgo la seguridad de la información por el bajo porcentaje de cumplimiento del 37.52%, según la tabla 4.1: Cumplimiento de los dominios

4.3.7. Dominio Seguridad en las Telecomunicaciones

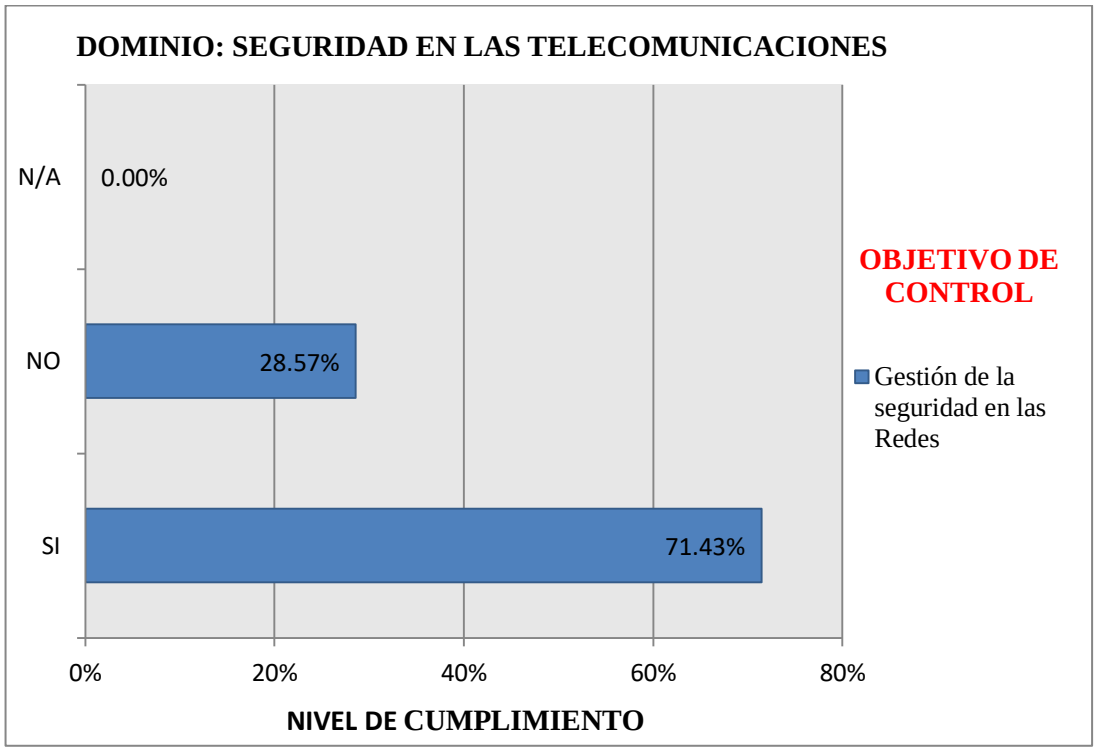

Gráfico 4. 9: Dominio Seguridad en las Telecomunicaciones
Elaboración propia

El objetivo de este dominio es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte. Según la norma ISO/IEC 27001, determina que deben cumplirse todas las acciones de control para minimizar los riesgos que pueda sufrir, pero se ha encontrado según el análisis realizado a la Universidad Nacional de Piura, que con respecto a este domino, es el único que tiene un porcentaje alto de cumplimiento, como se puede apreciar en el gráfico 4.9. Esto es debido a una cantidad considerable de controles implementados. Sin embargo, siguiendo los lineamientos de la norma técnica no es suficiente, puesto que se deben cumplir con todos los controles propuestos. Ante ello se puede apreciar una tabla resumen de los objetivos de control para conocer su cumplimento:

Tabla 4. 8: Resumen de los Objetivos de control del Dominio Seguridad en las Telecomunicaciones

Objetivos de control	Porcentaje de incumplimiento	Porcentaje de cumplimiento	N/A
Gestión en la seguridad en las redes	28.57%	71.43%	0.00%

Como se puede apreciar en la tabla 4.8, el porcentaje de cumplimiento del dominio es del 71.43%, es mayor a los demás dominios analizados, esto es favorable para la institución, debido a que si se ha establecido políticas sobre redes, se ha definido políticas sobre los puntos de acceso, si tienen mecanismo de autenticación de usuarios, si tienen herramientas de detección de Spyware/Spam y si tienen herramientas de detección de código malicioso. Sin embargo para que se reduzcan los riesgos, la norma establece que deben de cumplirse con todos los objetivos de control, poniendo atención al 28.57% restante.

Por lo tanto se concluye que el dominio debe implementar todos los controles propuestos para desear el objetivo deseado.

4.4. MODELAMIENTO DE LOS PROCESOS ACADÉMICOS

En el presente capítulo se muestra cómo se realizaron aquellos procesos que están involucrados en el alcance del SGSI, para ello, se efectuaron entrevistas con los encargados de los procesos para recolectar la información necesaria de su funcionamiento del trabajo en el área.

Para realizar el modelado de procesos, se decidió utilizar la notación BPMN 2.0 (Business Process Modeling Notation) a fin de facilitar la labor de análisis y evaluación de riesgos una vez identificados los activos involucrados al sistema, esto debido a que nos permite graficar una serie de eventos, definir los tipos de tareas con las que se está trabajando y asociar los activos identificados dentro del proceso a una tarea específica. Además permite observar de manera detallada todo el flujo de trabajo que siguen dichos procesos.

A continuación se procede a describir y detallar los procesos académicos de la Universidad Nacional de Piura de acuerdo al reglamento académico y las actualizaciones a la fecha. (Reglamento Académico de la Universidad Nacional de Piura, 2006).

4.4.1. Proceso de Calendarización Académica

Generar y registrar en el sistema la programación académica, (inicio de semestre) en consideración al Calendario Académico elaborado y aprobado por la Comisión Académica de la UNP, de manera oportuna para facilitar la planificación de las actividades académicas, y de soporte necesarias para una adecuada prestación del servicio educativo.

Responsables del Proceso

- Vicerrectorado Académico
- OCRA
- CIT

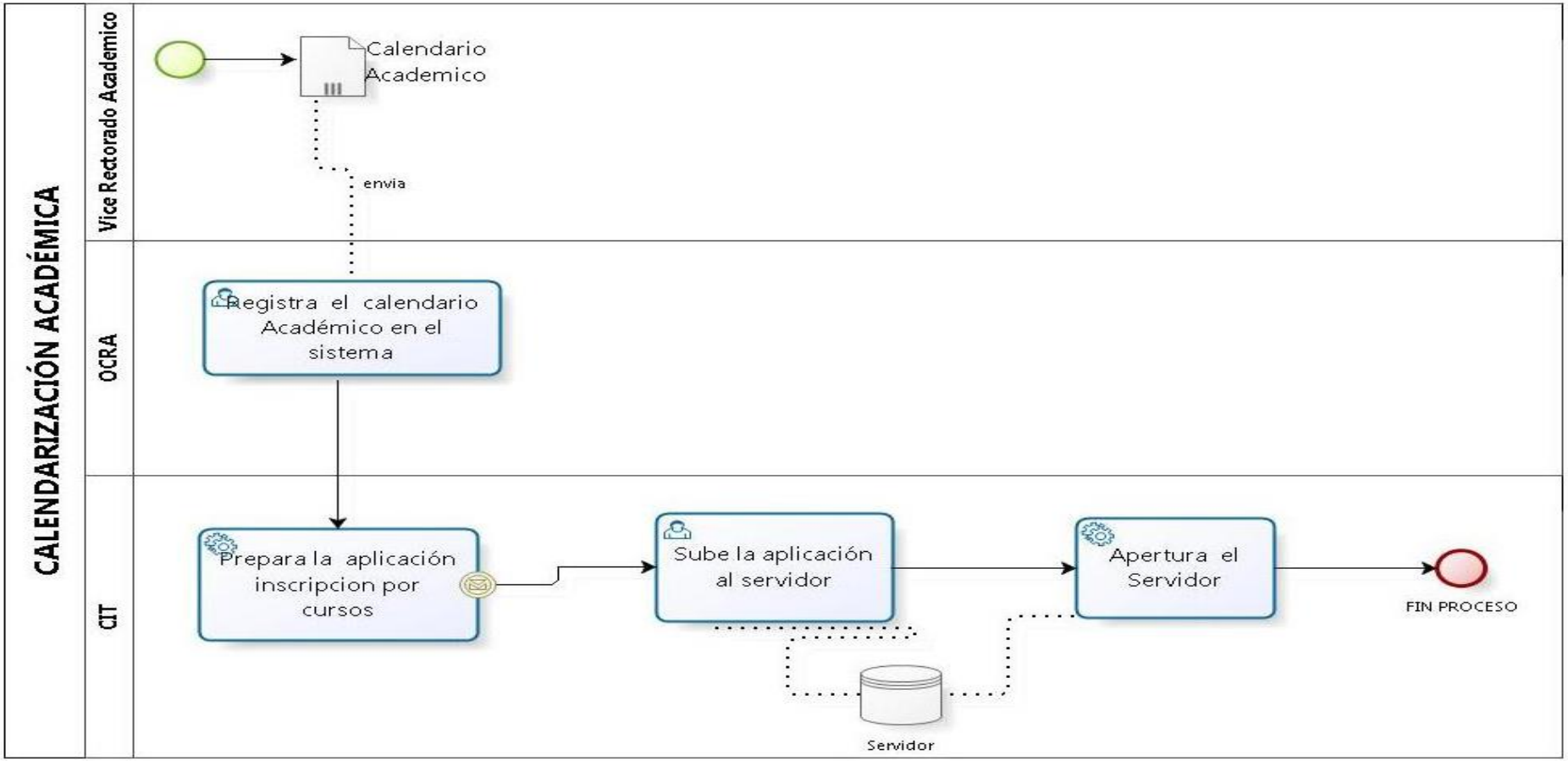

Gráfico 4. 10: Calendarización Académica

Elaboración propia.

4.4.2. Programación Académica de Cursos por Semestre.

Definir los cursos para cada ciclo académico teniendo en cuenta los cursos de ciclos pares e impares según el semestre que corresponda. Es responsabilidad de las Facultades de la UNP las cuales harán su Programación Académica de Cursos en coordinación con los Departamentos Académicos. La Programación Académica correspondiente a un determinado Ciclo Académico se dará a conocer por lo menos 6 semanas antes de terminar el semestre anterior. Designar a los docentes para el dictado de una asignatura, considerando el cumplimiento de perfiles docentes y los niveles de exigencia requeridos para cada asignatura.

Responsable del Proceso

- Facultades: (Director de Departamento, Director de Escuela y Secretario Académico).Ejecuta el proceso
- CIT: Da soporte al proceso**.**

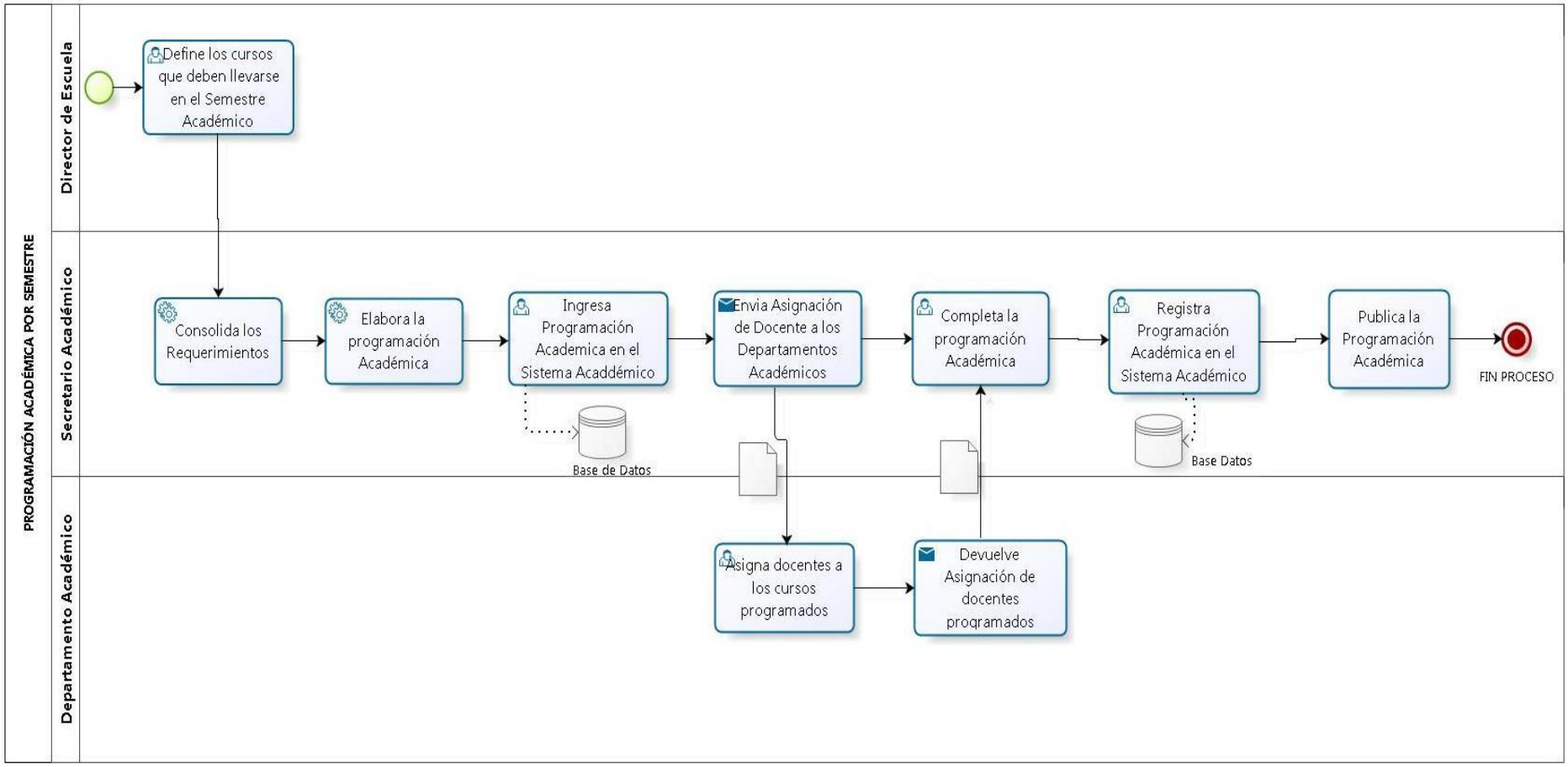

Gráfico 4. 11: Proceso Programación Académica por semestre

Elaboración propia

4.4.3. Proceso de Generación de Actas.

En la primera semana el docente registra en el Sistema Académico (Módulo REGEVA), los instrumentos de evaluación y fechas programadas en que serán aplicados y la ponderación de cada instrumento de evaluación, que permite el cálculo del promedio final. En el desarrollo del semestre académico, se debe registrar las calificaciones de los instrumentos, asistencias que han sido programados, considerando los plazos establecidos en la normativa. Finalizado el semestre o ciclo de clases, el docente genera un registro auxiliar y el acta, inmediatamente esa acta envía a través del Sistema Académico a la Oficina Central de Registro y Coordinación Académica (OCRA), para las gestiones correspondientes, la que las refrendará y devolverá una copia al Departamento Académico y el docente acudirá a firmar dicho documento.

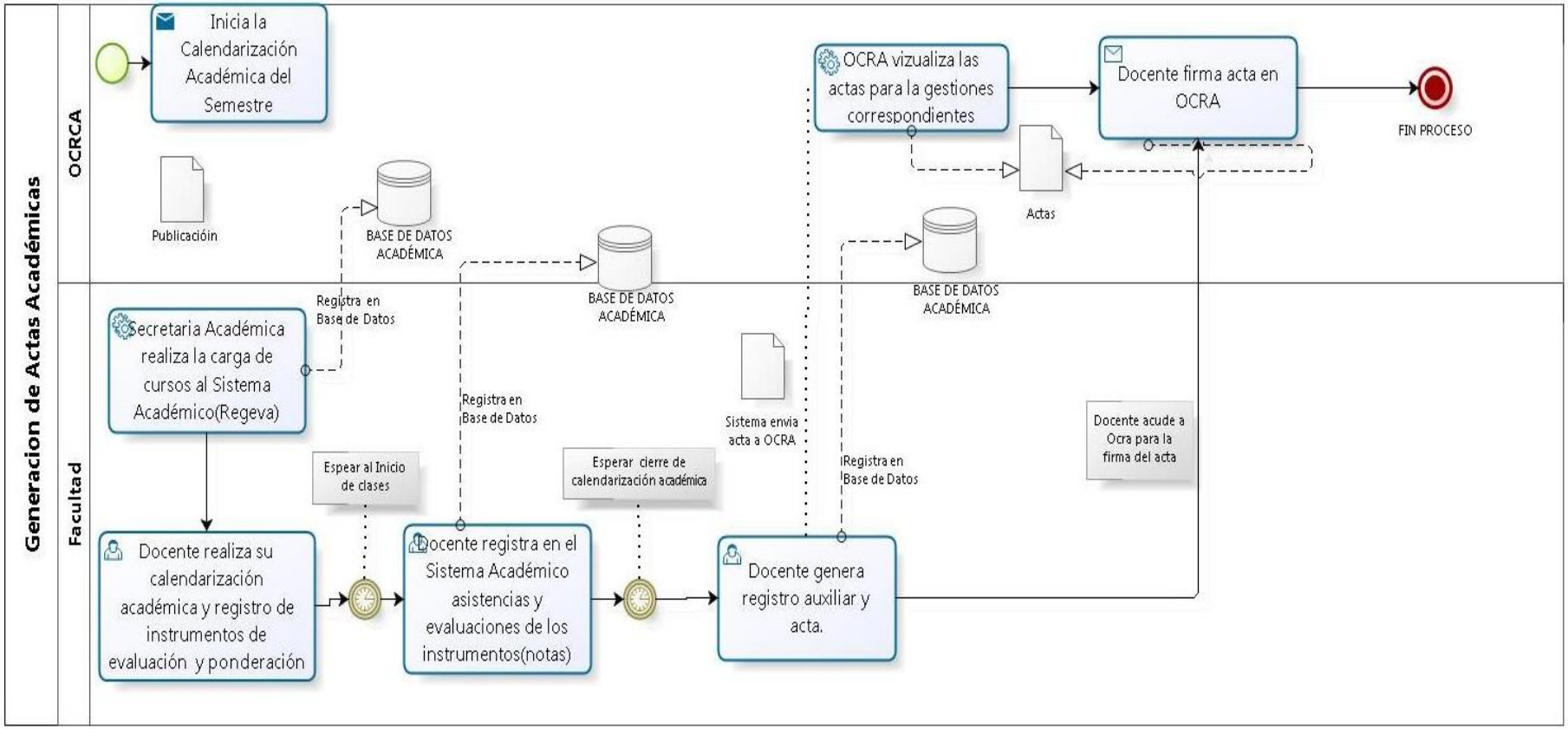

Gráfico 4. 12: Proceso Generación de Actas

Elaboración propia

4.4.4. Proceso de Modificación de Nota

El alumno que crea necesario presentar algún reclamo lo podrá hacer mediante dos modalidades:

1) Entrevista directa con el profesor del curso o Jefe de Prácticas.

2) Presentación de una solicitud dirigida al profesor del curso o Jefe de Prácticas, especificando la razón de su reclamo, adjuntando la práctica, paso o examen correspondiente; ésta será recepcionada por la secretaría del Departamento Académico y el Profesor tendrá un plazo de dos (02) días hábiles para expedir la respuesta.

Si el Profesor o Jefe de Prácticas no reconociera correcto el reclamo y el alumno mantuviera su posición, este último podrá presentar su reclamo al Director del Departamento Académico correspondiente, en sesión de Departamento se resolverá en última instancia, dentro de un plazo máximo de cinco (05) días hábiles, siendo esta decisión inimpugnable.

Responsable del Proceso

- Alumno
- Docente
- Director de Departamento

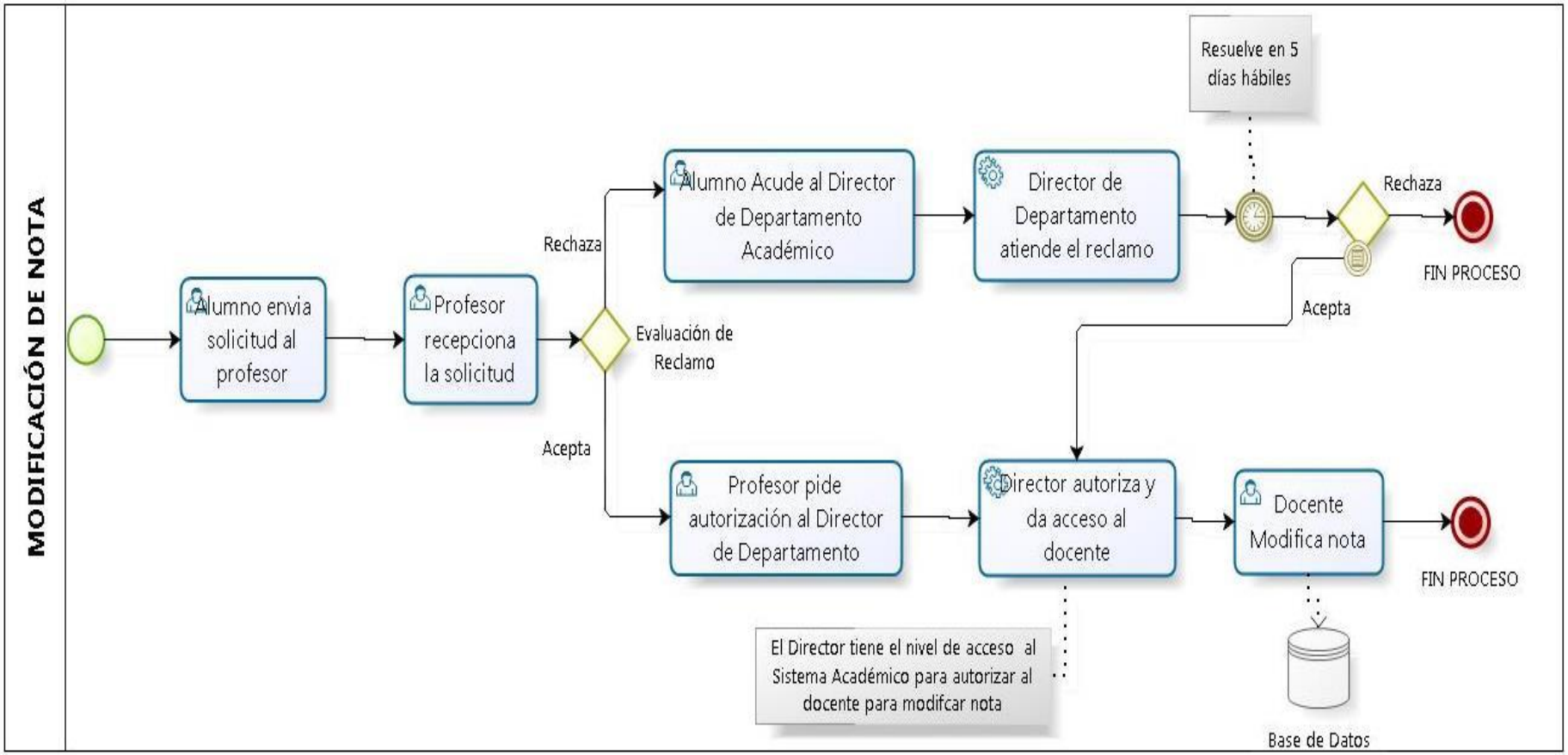

Gráfico 4. 13: Proceso Modificación de Notas

Elaboración propia

4.4.5. Proceso de Inscripción por curso.

La inscripción por cursos se realiza teniendo en consideración el Calendario Académico elaborado y aprobado por la Comisión Académica de la UNP. La inscripción por cursos (selección de cursos, nominaciones, códigos, claves, etc.) es personal y de exclusiva responsabilidad del alumno.Dentro de este proceso encontramos un Sub proceso de Soporte del CIT garantizando la operatividad del proceso. A continuación se muestra el proceso y subproceso mencionado:

Responsables del Proceso:

- CIT
- Alumno

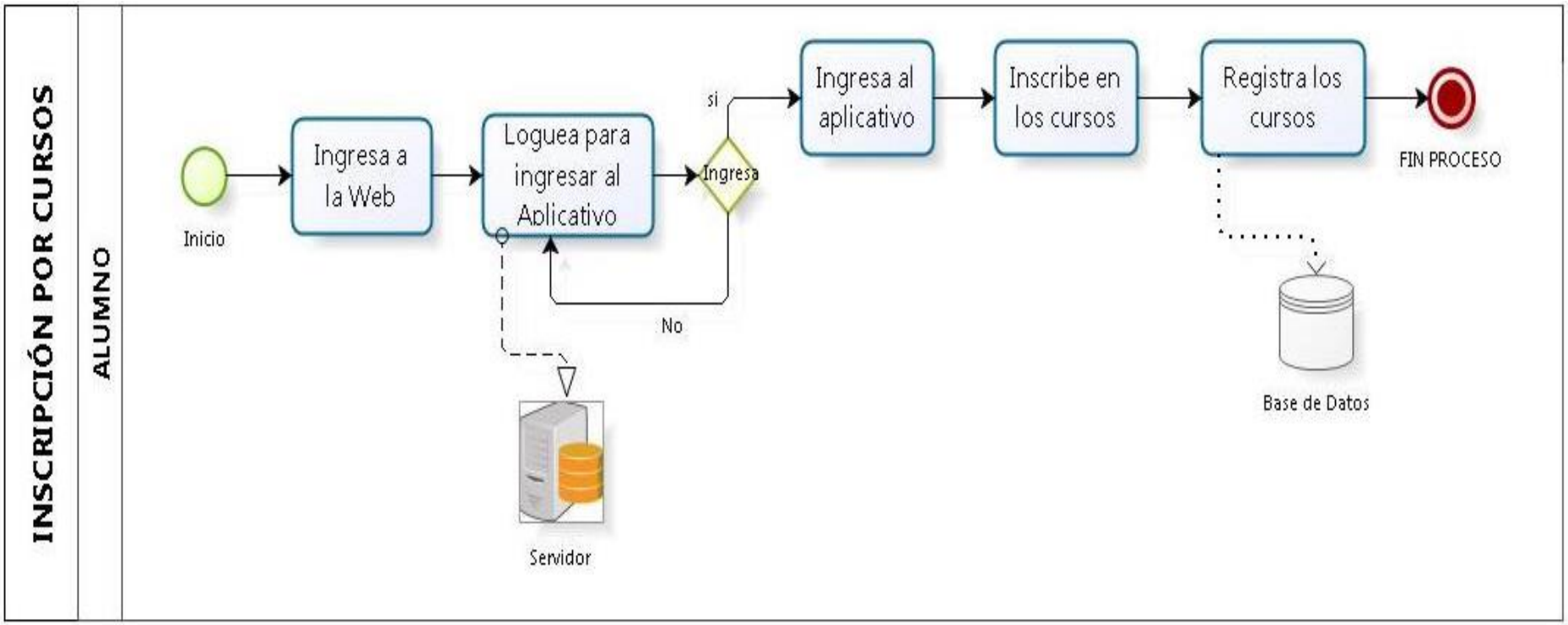

Gráfico 4. 14: Proceso Inscripción por Cursos

Elaboración propia

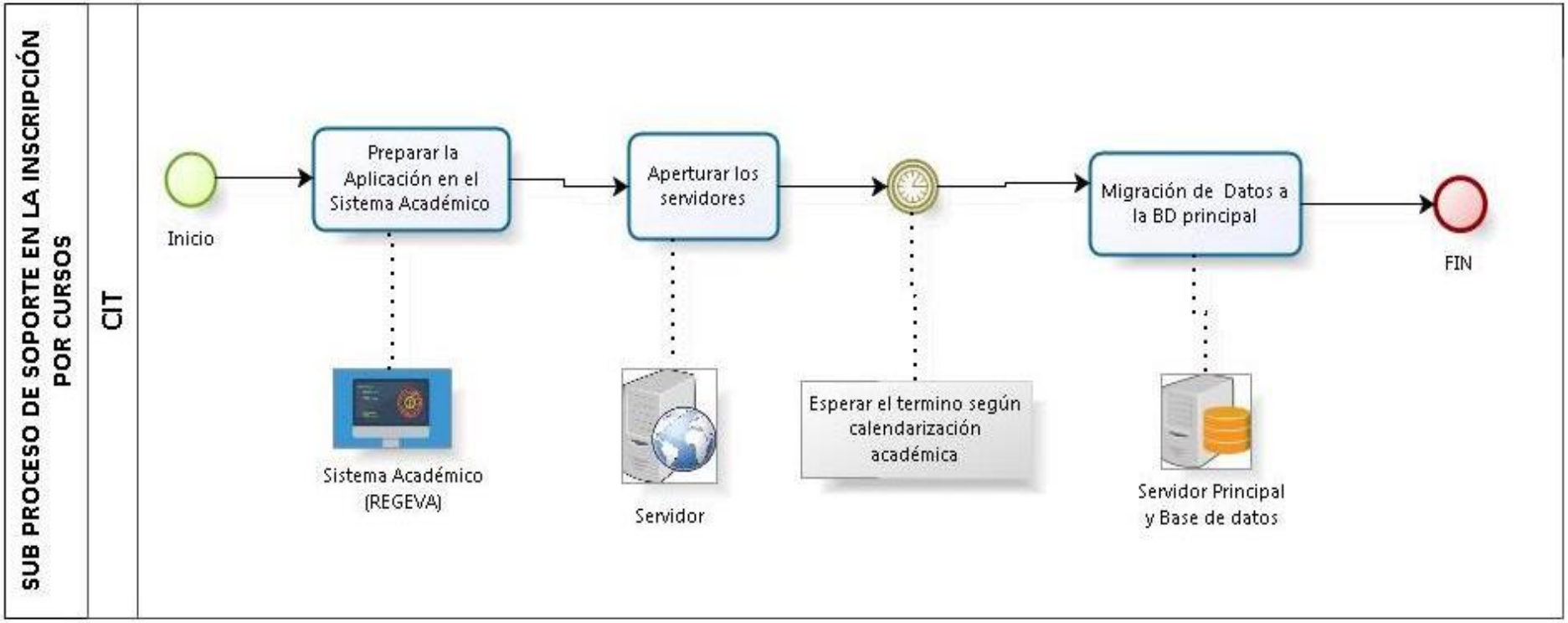

Gráfico 4. 15: Sub Proceso de Soporte en la Inscripción por cursos

Elaboración propia

4.4.6. Procesos de Soporte del CIT.

Las áreas del Centro de Información y Telecomunicaciones dan soporte a todo el Proceso académico, y además tienes procesos propios vinculados a la gestión educativa por tal motivo es importante conocer las acciones que realiza. A continuación se muestra en los siguientes gráficos:

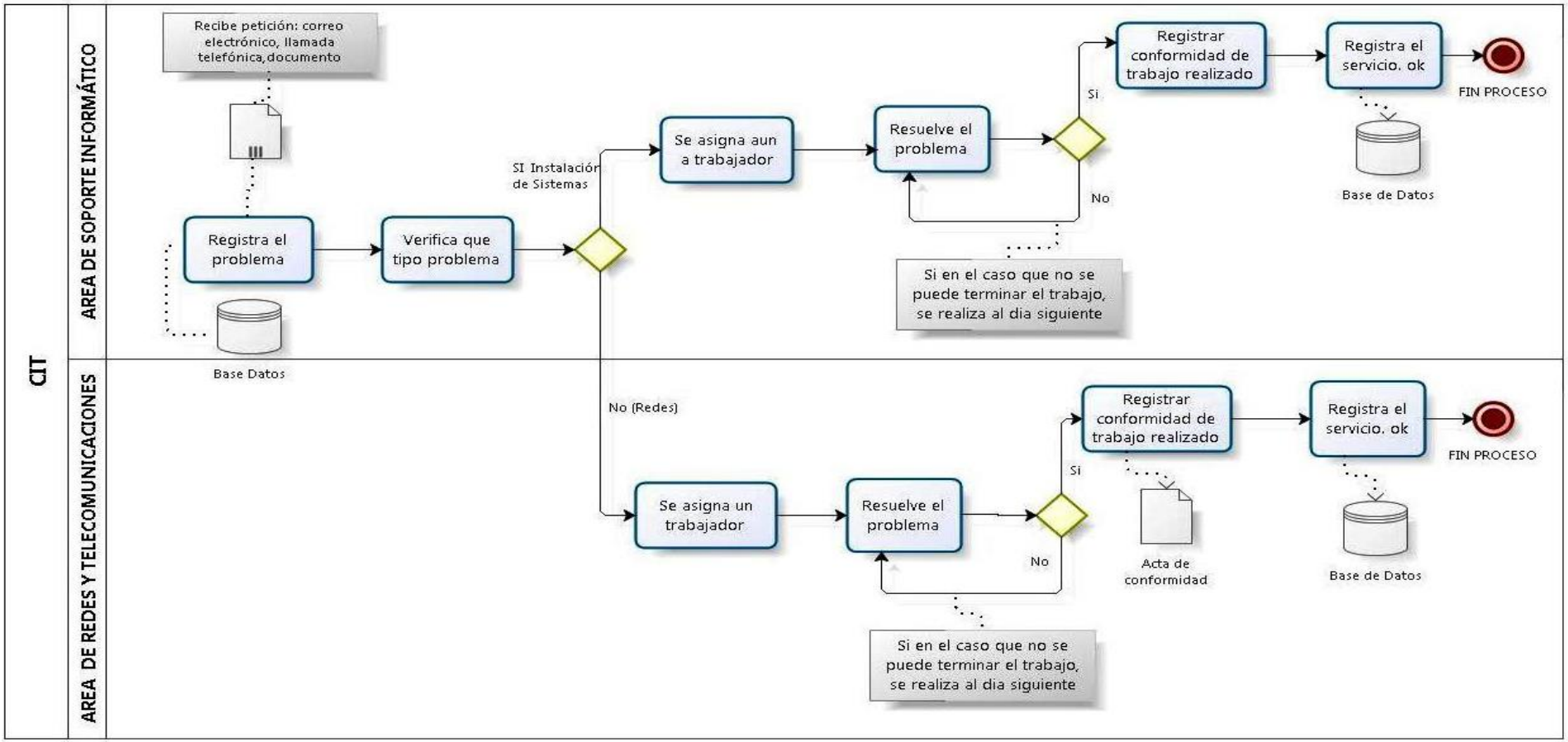

Gráfico 4. 16: Proceso de Soporte- CIT

Elaboración propia

4.4.7. Proceso de Desarrollo de Sistemas.

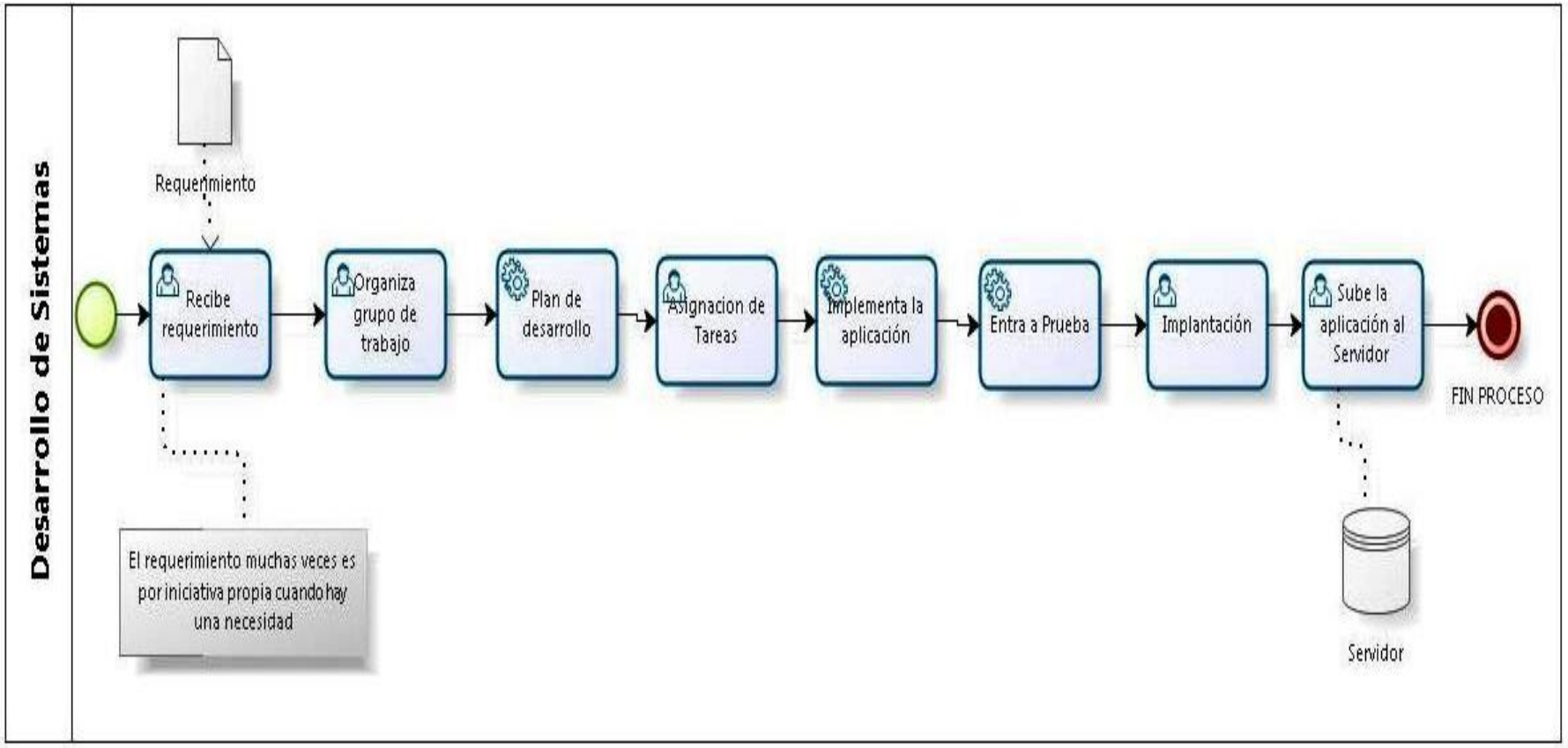

Gráfico 4. 17: Proceso Desarrollo de Sistemas – CIT

Elaboración propia

4.5. IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS

Una vez mapeado cada uno de los procesos que forman parte del alcance de la investigación, se recopiló información para identificar cada uno de los activos que están involucrados en los procesos, luego se procedió a valorarlos y asegurar cada uno de los activos más importantes para la institución.

4.5.1. Identificación

En este punto se identificaron los activos que están envueltos en cada proceso descrito anteriormente. Se organizaron reuniones paulatinas con los profesionales especialistas en tecnologías de información que trabajan en CIT, y docentes de la facultad de Ingeniería Industrial con el fin de generar y ajustar una lista de activos importantes para la institución. Según el estándar ISO 27005:2008, se pueden identificar dos tipos de activos: los primarios y los de soporte. Los primarios, según este estándar, son los procesos e información más sensibles para la organización. Los activos de soporte, son los activos que dan el debido soporte a estos activos primarios. Dentro de estas dos agrupaciones, se definieron siete distintos tipos específicos de activos:

1) Dato: Es toda aquella información que se genera, envía, recibe y gestionan dentro de la organización. Dentro de este tipo, podemos encontrar distintos documentos que la institución educativa gestiona dentro de sus procesos.

2) Aplicación: Todo aquel software que se utilice como soporte en los procesos.

3) Personal: Son todos los actores que se ven involucrados en el acceso y el manejo de una u otra manera a los activos de información de la organización.

4) Servicio: Son los servicios que alguna área de la organización suministra a otra área o entidades externas a la misma.

5) Tecnología: Es todo el hardware donde se maneje la información y las comunicaciones.

6) Instalación: Es cualquier lugar donde se alojan los activos de información. Este lugar o ambiente puede estar ubicado dentro de la organización tanto como fuera de la misma.

7) Equipamiento auxiliar: Son los activos que no se hallan definidos en ninguno de los anteriores tipos.

A continuación, se muestra el inventario de todos los activos que se pudieron identificar dentro de los procesos académicos que se encuentran en el alcance del presente proyecto.

Tabla 4. 9: Inventario de Activos de la Universidad Nacional de Piura

Nombre del activo	Proceso	Tarea/Actividad	Tipo	Sub Tipo	Ubicación	Propietario	¿Quién usa el activo?	Medio de almacena-miento.	Tangible/ intangible
Backup de Base de Datos Académico de Producción	Proceso de Desarrollo de Sistemas	Generación de Backus del Sistema Académico de la Universidad	Soporte	Aplicación	DataCenter	Área de Desarrollo de Sistemas	Área de Desarrollo de Sistemas	Servidor de base de Datos	Intangible
Historiales Académicos	- Proceso de Generación de Actas. -Proceso de Inscripción por ciclo	Reporte de los historiales impresos obtenidos mediante el sistema a Académico	Primario	Dato	Armarios	Secretarios Académi-cos	-OCRA Vicerrectorado Académico -Área de Desarrollo de Sistemas del CIT -Decano -Alumno	Impreso	Tangible
Certificados de Estudios	- Proceso de Generación de Actas.	Reporte de los certificados impresos obtenidos mediante el sistema Académico	Primario	Dato	Armarios	Secretarios Académi-cos	-OCRA -Área de Desarrollo de Sistemas del CIT -Decano -Alumno	Impreso	Tangible
Informes Académicos	- Proceso de Generación de Actas.	Reporte de los informes impresos obtenidos mediante el	Primario	Dato	Armarios	Secretarios Académi-cos	-OCRA Vicerrectorado Académico -Área de Desarrollo de	Impreso	Tangible

		sistema Académico					Sistemas del CIT. -Decano de facultad -Alumno		
Ficha de Inscripción por cursos	- Proceso de Generación de Actas. -Proceso de Inscripción por ciclo	Reporte de la ficha de inscripción del estudiante obtenido mediante el sistema Académico	Primario	Dato	Armarios	Secretarios Académi-cos	-Área de Desarrollo de Sistemas del CIT -Decano de facultad -Alumno	Impreso	Tangible
Datos de Actas Promocionales	-Proceso generación de Actas	Generadas por el Sistema informático	Primario	Equipamiento auxiliar	DataCenter	Secretarios Académi-cos	- OCRA -Área de Desarrollo de Sistemas del CIT -Decano de facultad	Servidor de base de Datos	Intangible
Datos de Matriculas e Inscripciones	Proceso de Matrícula	Generadas por el Sistema informático	Primario	Equipamiento auxiliar	DataCenter	Secretarios Académi-cos	-OCRA -Área de Desarrollo de Sistemas del CIT -Decano de facultad	Servidor de base de Datos	Intangible
Datos de Notas Promocionales de Alumnos por Curso	Proceso generación de Actas	Generadas por el Sistema informático	Primario	Equipamiento auxiliar	DataCenter	Secretarios Académi-cos	-OCRA -Área de Desarrollo de Sistemas del CIT -Decano de facultad	Servidor de base de Datos	Intangible
Reglamento Académico	Programa-ción Académica	Documento impreso de normativa académica de	Primario	Dato	Armarios	-OCRA Vicerrecto-rado Académico	-OCRA Vicerrectorado académico -Decano de	Impreso	Tangible

		la Universidad				Decano de facultad Secretarios Académi-cos	facultad		
Estatuto de la Universidad Nacional de Piura	Programa-ción Académica	Documento impreso de normativa estatutaria de la Universidad	Primario	Dato	Armarios	-OCRA Vicerrecto-rado Académico -Decano de facultad Secretarios Académi-cos	-OCRA Vicerrectorado académico -Decano de facultad	Impreso	Tangible
Manual de Usuario del Sistema Académico	Todos los procesos académicos	Documento de referencia para el manejo del Sistema Académico en formato impreso o digital	Primario	Dato	Armarios	Desarrollo de Sistemas del CIT	-OCRA Vicerrectorado académico -Decano de facultad -Secretarios Académicos	Impreso	Tangible
Actas de Notas	Proceso generación de Actas	Reporte del acta de notas del docente obtenido mediante el sistema Académico	Primario	Dato	Armarios	Secretarios Académi-cos	.-OCRA Vicerrectorado Académico -Área de Desarrollo de Sistemas del CIT -Decano de facultad	Impreso	Tangible
Boleta de Notas Académicas	Proceso generación de Actas	Reporte de la boleta de notas del estudiante	Primario	Dato	Armarios	Secretarios Académico s	-Área de Desarrollo de Sistemas del CIT	Impreso	Tangible

por alumno		obtenido mediante el sistema Académico					-Decano de facultad -Alumno		
Listado de Modificacio-nes autorizadas de notas	-Proceso generación de Actas -Proceso de modificació n de notas	Reporte de modificaciones de notas obtenido mediante procesos de control	Primario	Dato	Armarios	Secretarios Académico s	-OCRA -Vicerrectorado Académico -Área de Desarrollo de Sistemas del CIT -Decano de facultad	Impreso	Tangible
Listado de Inscritos por cursos y secciones	Proceso de inscripción de cursos por ciclo	Listado de alumnos inscritos mediante el sistema Académico	Primario	Dato	Armarios	Secretarios Académico s	-Área de -Desarrollo de Sistemas -Decano de facultad	Impreso	Tangible
Bitácora de cambios en las aplicaciones	Proceso de Desarrollo de Sistemas	Documento de seguimiento a los cambios realizados al código fuente y procesos del aplicativo	Primario	Dato	Armarios	Área de Desarrollo de Sistemas del CIT	Área de Desarrollo de Sistemas del CIT	Impreso	Tangible
Base de Datos de Desarrollo	Proceso de Desarrollo de Sistemas	Grabación y actualización de la data académica de la Universidad	Soporte	Aplicación	Datacenter	Área de Desarrollo de Sistemas de CIT	Área de Desarrollo de Sistemas del CIT	Servidor de base de Datos	Intangible
Backup de Base de Datos de Producción	Proceso de Desarrollo de Sistemas	Generación de backups diarios del sistema	Soporte	Aplicación	Datacenter	Área de Desarrollo de Sistemas de CIT	Área de Desarrollo de Sistemas del CIT	Servidor de base de Datos	Intangible

		académico							
Backup de Base de Datos de Producción en Aplicativos Web	Proceso de Desarrollo de Sistemas	Generación de backup diarios de la data de los sistemas web académicos	Soporte	Aplicación	Datacenter	Área de Desarrollo de Sistemas de CIT	Área de Desarrollo de Sistemas del CIT	Servidor de base de Datos	Intangible
Código Fuente Aplicativos Desktop	Proceso de Desarrollo de Sistemas	Generación de código fuente de los aplicativos desarrollados en lenguaje de programación	Soporte	Aplicación	Datacenter	Área de Desarrollo de Sistemas de CIT	Área de Desarrollo de Sistemas del CIT	Servidor de aplicacio-nes. CD	Tangible
Claves cifradas de sistema informático	Proceso de Desarrollo de Sistemas	Generadas por el Sistema informático	Soporte	Aplicación	Datacenter	Área de Desarrollo de Sistemas de CIT	Área de Desarrollo de Sistemas del CIT	Servidor de aplicacio-nes. CD	Intangible
Contraseñas de empleados	Proceso de Desarrollo de Sistemas	Generadas por el Sistema informático	Soporte	Aplicación	Datacenter	Área de Desarrollo de Sistemas de CIT	-OCRA -Vicerrectorado Académico -Área de Desarrollo de Sistemas del CIT -Decano de facultad -Alumno	Servidor de aplicacio-nes. CD	Intangible
Código Fuente de Aplicativos Web	Proceso de Desarrollo de Sistemas	Generación de código fuente de los aplicativos desarrollados	Soporte	Aplicación	Datacenter	Área de Desarrollo de Sistemas de CIT	Área de Desarrollo de Sistemas del	Servidor de aplicacio-nes CD	Tangible

		en lenguaje de programación web							
CD de Backup de Produccion	Proceso de Desarrollo de Sistemas	Generación y grabado del backup en el medio físico	Soporte	Tecnología	Datacenter	Área de Desarrollo de Sistemas de CIT	Área de Desarrollo de Sistemas del	CD	Tangible
Herramientas de Desarrollo	Proceso de Desarrollo de Sistemas	Lenguajes de programación que se utiliza para los aplicativos.	Soporte	Aplicación	Desarrollo de Sistemas	Área de Desarrollo de Sistemas de CIT	Procesos de Soporte CIT Área de Desarrollo de Sistemas del	CD	Tangible
Licencia SQL Server	Procesos de Soporte CIT	Licencia del gestor de BD de producción y pruebas	Soporte	Aplicación	Datacenter	Área de Soporte Técnico CIT	Procesos de Soporte CIT	CD	Tangible
Licencia .Net	Procesos de Soporte CIT	Lenguaje de programación para las aplicaciones Web	Soporte	Aplicación	Datacenter	Área de Soporte Técnico CIT	Procesos de Soporte CIT	CD	Tangible
Sistema Operativo de Servidor Windows Server 2013	Procesos de Soporte CIT	Sistema operativo de soporte a la base de Datos y servidores de aplicaciones	Soporte	Aplicación	Datacenter	Área de Soporte Técnico CIT	Procesos de Soporte CIT	CD	Tangible
Antivirus Eset ENDPOINT Security	Procesos de Soporte CIT	Antivirus legalizado por la universidad para sus servidores	Soporte	Aplicación	Datacenter	Área de Soporte Técnico CIT	-OCRA -Vicerrectorado Académico -Área de Desarrollo de Sistemas del CIT -Decano de	CD	Tangible

							facultad		
Servidor de Aplicaciones Web	Soporte Aplicación	Hardware donde se soporta las aplicaciones Web	Soporte	Tecnología	Datacenter	Área de Soporte Técnico CIT	Área Redes y Telecomunicaciones	Servidor	Tangible
Servidor de Aplicaciones Desktop	Procesos de Soporte CIT	Hardware donde se soporta las aplicaciones Desktop	Soporte	Tecnología	Datacenter	Área de Soporte Técnico CIT	Área Redes y Telecomunicacio-nes	Servidor	Tangible
PC de Desarrollo	Proceso de Desarrollo de Sistemas	Computadoras de escritorio donde se realizan tareas de desarrollo de sistemas, mantenimiento y reportes	Soporte	Tecnología	Oficina de Desarrollo	Área de Desarrollo de Sistemas de CIT	Área de Desarrollo de Sistemas de CIT	--------	Tangible
DataCenter	Procesos de Soporte CIT	Ambiente donde se encuentra almacenado todos los datos de la Institución	Soporte	Tecnología	----------	Área Redes y Telecomunicaciones	Área Redes y Telecomunica-ciones	----------	
Diseño de infraestructu-ra de red	Procesos de Soporte CIT	Servicios de TI	Soporte	Dato	----------	-Área Redes y Telecomunicaciones	Área Redes y Telecomunica-ciones	Planos	Tangible
Switch, Enrutadores, Conmutadores de red	Procesos de Soporte CIT	Servicios de TI	Soporte	Tecnología	OCRA Vicerrectorado Académico	- Área Redes y Telecomunicaciones	Área Redes y Telecomunica-ciones	----------	Tangible

					CIT Facultades	-OCRA - Vicerrecto-rado Académico -Facultades			
Fuentes de alimentación	Procesos de Soporte CIT	Servicios de TI	Soporte	Tecnología	Oficinas, DataCenter	OCRA - Vicerrecto-rado Académico -Área de Desarrollo de Sistemas del CIT -Decano de facultad	-OCRA -Vicerrectorado Académico -Área de Desarrollo de Sistemas del CIT -Decano de facultad	----------	Tangible
Sistemas de alimentación ininterrumpi-da	Procesos de Soporte CIT	Servicios de TI	Soporte	Tecnología	DATA CENTER	Área Redes y Telecomu-nicaciones	Área Redes y Telecomunica-ciones	----------	Tangible
Sistemas contra incendios	Procesos de Soporte CIT	Servicios de TI	Soporte	Tecnología	DATA CENTER TODAS LAS AREAS	Área Redes y Telecomu-nicaciones	-OCRA -Vicerrectorado Académico -Facultades	----------	Tangible
Sistemas de aire acondiciona-do	Procesos de Soporte CIT	Servicios de TI	Soporte	Tecnología	DATA CENTER	Área Redes y Telecomu-nicaciones	----------	----------	Tangible
Sistemas de filtrado de aire	Procesos de Soporte CIT	Servicios de TI	Soporte	Tecnología	DATA CENTER	Área Redes y Telecomu-nicaciones	----------	----------	Tangible

Identificadores biométricos de los empleados	Procesos de Soporte CIT	Servicios de TI	Soporte	Tecnología	CIT	Área Redes y Telecomu-nicaciones	-CIT	----------	Tangible
Correo electrónico	Procesos de Soporte CIT	Servicios de TI	Soporte	Aplicación	Todas las Áreas	Área Redes y Telecomu-nicaciones	Todas las Áreas	----------	Intangible
Mensajería instantánea	Procesos de Soporte CIT	Servicios de TI	Soporte	Aplicación	Todas las Áreas	Área Redes y Telecomu-nicaciones	Todas las Áreas	----------	Intangible
Microsoft Outlook® Web Access (OWA)	Procesos de Soporte CIT	Servicios de TI	Soporte	Aplicación	Todas las Áreas	Área Redes y Telecomu-nicaciones	Todas las Áreas	----------	Intangible
Microsoft Active Directory®	Procesos de Soporte CIT	Servicios de TI	Soporte	Aplicación	Red Local	Área Redes y Telecomu-nicaciones	Área Redes y Telecomunica-ciones	Servido-res de Active Directory	Intangible
Sistema de nombres de dominio (DNS)	Procesos de Soporte CIT	Servicios de TI	Soporte	Aplicación	Red Local	Área Redes y Telecomu-nicaciones	Área Redes y Telecomunica-ciones	Servidor DNS	Intangible
Protocolo de configuración dinámica de host (DHCP)	Procesos de Soporte CIT	Servicios de TI	Soporte	Aplicación	Red Local	Área Redes y Telecomu-nicaciones	Área Redes y Telecomunica-ciones	Servidor DHCP	Intangible
Recursos (Impresoras, fax, etc.)	Todos los procesos	Servicios de TI	Soporte	Tecnología	Red Local	-Área Redes y Telecomu-nicaciones	Todas las áreas	----------	Tangible

						-OCRA Vicerrecto-rado Académico -Facultades			
Acceso de Administración remota	Procesos de Soporte CIT	Servicios de TI	Soporte	Aplicación	Red Local	Área Redes y Telecomu-nicaciones	Área Redes y Telecomunica-ciones	----------	Intangible
Acceso a red privada virtual (VPN)	Procesos de Soporte CIT	Servicios de TI	Soporte	Aplicación	Red Local	Área Redes y Telecomu-nicaciones	Todas las áreas	VPN	Intangible
Dispositivo firewall de hardware y software	Procesos de Soporte CIT	Servicios de TI	Soporte	Tecnología	Redes	Área Redes y Telecomu-nicaciones	Área Redes y Telecomunica-ciones	----------	Tangible Intangible
PC de escritorio	Todos los procesos	Computadoras de escritorio donde se realizan tareas académicas	Soporte	Tecnología	Oficinas	-OCRA Vicerrecto-rado -Facultades	Todas las áreas	----------	Tangible
Software de oficina	Todos los procesos	Aplicaciones de oficina escritorio donde se realizan tareas académicas.	Soporte	Tecnología	Pc de oficina	-OCRA Vicerrecto-rado -Facultades	Todas las áreas	----------	Tangible

Fuente: Centro de Informática y Telecomunicaciones de la UNP

4.5.2. Valorización de los activos de información.

El siguiente paso a la identificación de los activos que se encuentren comprendidos dentro de los procesos del Universidad Nacional de Piura es valorizarlos, y así determinar el valor que cada activo tiene para la institución y el impacto que tendría dentro de la misma si llegara a fallar en algún momento.

Para realizar dicha valorización, se utilizó la metodología de Identificación y Valoración de activos y Valoración de impactos del anexo B de la ISO/IEC 27005:2008 recomendada por la ISO/IEC 270001. En ella se determinó una escala cualitativa ya que no es posible valorar económicamente todos los activos envueltos dentro de estos procesos. En la siguiente tabla se muestra cuáles son los criterios que se usaron para realizar la correcta valorización de estos activos, en conjunto con los valores que se tendrán en cuenta para clasificarlos y su respectivo significado dentro del contexto actual:

Tabla 4. 10: Criterio de Valoración

CRITERIO	VALOR	DESCRIPCION
Disponibilidad	0	No Aplica / No es relevante
	1	Debe estar disponible al menos el 10% del tiempo
	2	Debe estar disponible al menos el 50% del tiempo
	3	Debe estar disponible siempre
Integridad	0	No Aplica / No es relevante
	1	No es relevante los errores que tenga o la información faltante
	2	Tiene que estar correcto y completo al menos en un 50%
	3	Tiene que estar correcto y completo en un 100%
Confidencialidad	0	No Aplica / No es relevante
	1	Daños muy bajos, el incidente no trascendería del área afectada
	2	Seria relevantes, el incidente implicaría a otras áreas
	3	Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas

Fuente: la ISO/IEC 27005:2008

Para hallar el valor final del activo, se realizó una suma de los valores de los distintos criterios. Esta suma se ubicará en el rango de valores de 0 a 9, para lo cual cada valor representará a un nivel de criticidad. Mientras más alto sea el número final que resultó de la suma, más alta será su criticidad. Para esta investigación, se definieron cuatro niveles de criticidad del activo: no aplica, bajo, medio y alto. A continuación, la siguiente tabla detalla los valores que se puede obtener, asociados a un nivel de criticidad específico.

Tabla 4. 11 Nivel de Criticidad

VALOR	CRITICIDAD
0	No Aplica
1	Baja
2	Baja
3	Baja
4	Medio
5	Medio
6	Medio
7	Alta
8	Alta
9	Alta

Fuente: ISO/IEC 27005:2008

4.5.3. Apetito del riesgo

Se definió que los activos cuya criticidad sea “Alta” son los que entrarán dentro de la identificación y análisis de riesgos de los activos de información del siguiente capítulo. Los activos con criticidad “Media” y “Baja” no se toman como activos críticos para la institución, por lo cual no entraron dentro de dicho análisis Luego de haber definido el contexto de la valorización, se procedió a mostrar el total de los activos identificados con el valor respectivo que cada activo tiene dentro de la institución. A continuación se puede apreciar la tabla 4.5: Matriz de Valoración de Activos.

Tabla 4. 12: Matriz de Valoración de Activos

ID	ACTIVO	CRITERIOS DE VALORACION			VALOR	CRITICIDAD
		INTEGRIDAD	DISPONIBILIDAD	CONFIABILIDAD		
1	Backup de Base de Datos Académico de Producción	3	3	3	9	Alta
2	Historiales Académicos	3	3	3	9	Alta
3	Certificados de Estudios	3	3	3	9	Alta
4	Informes Académicos	3	3	3	9	Alta
5	Ficha de Datos personales del Estudiante	3	3	2	8	Alta
6	Ficha de Inscripción por cursos	3	3	2	8	Alta
7	Datos de Actas Promocionales	3	3	3	9	Alta
8	Datos de Matriculas e Inscripciones	3	3	3	9	Alta
9	Datos de Notas Promocionales de Alumnos x Curso	3	3	3	9	Alta
10	Reglamento Académico	3	3	3	9	Alta
11	Estatuto de la Universidad Nacional de Piura	3	3	3	9	Alta
12	Manual de Usuario del Sistema Académico	3	3	3	9	Alta
13	Actas de Notas	3	3	3	9	Alta
14	Boleta de Notas Académicas por alumno	3	3	3	9	Alta
15	Listado de Modificaciones autorizadas de notas	0	1	2	3	Baja
16	Listado de Inscritos por cursos y secciones	3	3	2	8	Alta
17	Bitácora de cambios en las aplicaciones	3	3	2	8	Alta
18	Base de Datos de Desarrollo	3	3	3	9	Alta
19	Backup de Base de Datos de Producción	3	3	3	9	Alta
20	Backup de Base de Datos de Producción en Aplicativos Web	3	3	3	9	Alta
21	Código Fuente Aplicativos Desktop	3	3	3	9	Alta

22	Claves cifradas de sistema informático	3	3	2	8	Alta
23	Contraseñas de empleados	3	3	2	8	Alta
24	Código Fuente de Aplicativos Web	3	3	3	9	Alta
25	CD de Backup de Producción	3	3	2	8	Alta
26	Herramientas de Desarrollo	3	3	1	7	Alta
27	Licencia SQL Server	3	2	2	7	Alta
28	Licencia .Net	3	2	2	7	Alta
29	Sistema Operativo de Servidor Windows Server 2013	2	3	2	7	Alta
30	ANTIVIRUS ESET ENDPOINT SECURITY	3	3	2	8	Alta
31	Servidor de Aplicaciones Web	3	3	3	9	Alta
32	Servidor de Aplicaciones Desktop	3	3	3	9	Alta
33	PC de Desarrollo	3	3	2	7	Alta
34	DataCenter	3	3	3	9	Alta
35	Diseño de infraestructura de red	3	2	2	7	Alta
36	Switch, Enrutadores, Conmutadores de red	3	3	3	7	Alta
37	Fuentes de alimentación	3	3	2	7	Alta
38	Sistemas de alimentación ininterrumpida	3	3	3	8	Alta
39	Sistemas contra incendios	3	3	2	7	Alta
40	Sistemas de aire acondicionado-	3	3	2	7	Alta
41	Sistemas de filtrado de aire	3	3	2	7	Alta
42	Identificadores biométricos de los empleados	3	3	2	7	Alta
43	Correo electrónico	3	3	2	7	Alta
45	Microsoft Outlook® Web Access (OWA)	3	3	2	5	Media
45	Microsoft Active Directory®	3	3	2	7	Alta
46	Sistema de nombres de dominio (DNS)	3	3	2	7	Alta
47	Protocolo de configuración dinámica de host (DHCP)	3	3	2	7	Alta
48	Uso compartido de Recursos (Impresoras, fax, etc.)	3	2	2	4	Media

49	Acceso a red privada virtual (VPN)	3	3	3	7	Alta
50	Dispositivo firewall de hardware y software	3	3	3	7	Alta
51	Cableado de red	3	3	3	8	Alta
52	Fibra Óptica	3	3	3	8	Alta
53	PC de oficina	3	3	1	7	Alta

Fuente: ISO/IEC 27005:2008

4.6. IDENTIFICACIÓN Y EVALUACIÓN DE LOS RIESGOS

El objetivo es la elaboración de la Matriz de Riesgos de la institución, para ello se definió una metodología de evaluación de riesgos, en la cual se describía cual era el apetito de riesgo de la organización, el procedimiento para la identificación de riesgos y el criterio para la evaluación de los mismos.

Para el desarrollo de esta metodología se utilizó la norma ISO/IEC 27005:2008, la cual brinda una guía sobre la gestión de riesgos en la seguridad de la información, y se adaptó según las necesidades de la institución, esta metodología puede encontrarse en los documentos de la ISO: Metodología de Análisis de Riesgos del ISO/IEC 27005:2005. Los pasos involucrados dentro de ella son:

4.6.1. Identificación del Riesgo

El primer paso dentro de la metodología es la identificación de las amenazas y vulnerabilidades, para ello, se deberá escoger aquellos activos de información que fueron considerados los más importante en la identificación y valoración de activos y se evaluará a que amenazas y vulnerabilidades se encuentran expuestas.

Para realizar este trabajo de identificación de riesgos, es necesario definir lo que es una amenaza, vulnerabilidad y riesgo. En la metodología de evaluación se define a las amenazas como aquellos eventos o actividades que pueden dañar o afectar a los activos de información.

Las vulnerabilidades no pueden dañar a los activos por si solos, ya que son características propias de estos; sin embargo, deben ser identificadas debido a que son fuentes potenciales de riesgos en caso logren ser explotadas por alguna amenaza.

Por último, los riesgos se definieron como aquella probabilidad de que una amenaza explote alguna vulnerabilidad haciéndole perder alguna propiedad relacionada a la seguridad de la información (confidencialidad, disponibilidad, integridad y auditabilidad.), de ahí la necesidad de identificar las amenazas y vulnerabilidades previamente.

Se utilizó una lista de ejemplos de vulnerabilidades y amenazas proporcionadas por la ISO/IEC 27005:2008, la cual se puede visualizar en el Anexo Nº3 : Lista de Ejemplos de Vulnerabilidades y Amenazas.

4.6.2. Evaluación del valor de riesgo.

Una vez identificados los riesgos, se procedió a evaluar, junto con los dueños de los procesos, cuáles son las probabilidades de ocurrencia y los impactos que traerían a la organización en caso se materialicen estos riesgos, para ello podrán usar las escalas desde "Muy Baja" hasta "Muy Alta" para las probabilidades y una escala de "Insignificante" hasta "Catastrófica" para el impacto.

A continuación se presentan las tablas con las escalas de valoración de probabilidades e impactos y el criterio utilizado

Tabla 4. 13: Lista de Probabilidades

LISTA DE PROBABILIDADES			
Nivel	Descripción	Escala de porcentaje	Probabilidad
5	Muy Alta	Más de 80%	Ocurrirá en la mayoría de las circunstancias; todos los días o varias veces al mes.
4	Alta	60% -80%	Probablemente ocurrirá en la mayoría de las circunstancias; al menos una vez al mes.
3	Moderada	40% - 60%	Puede ocurrir en algún momento; al menos una vez al año.
2	Baja	20% - 40%	Podría ocurrir en algún momento; al menos una vez cada dos años
1	Muy Baja	Menos de 20%	Puede ocurrir en circunstancias excepcionales; como dos veces cada cinco años.

Fuente: ISO/IEC 27005:2008

Tabla 4. 14. Lista de Niveles de Impacto

LISTA DE NIVELES DE IMPACTO		
Nivel	Descriptivo	Explicación
8	Catastrófica	Pérdida o daño catastrófico a la reputación de la institución; pérdidas financieras importantes, intervención regulatoria con sanciones por faltas muy graves; involucramiento directo de la alta gerencia o directorio. Afecta por más de una semana las operaciones.
6	Mayor	Daño sobre la institución es mayor, riesgo inusual o inaceptable y sanciones por falta grave; involucramiento de la alta gerencia, gastos operativos de consideración.. Afecta hasta en 72 horas las operaciones
4	Moderado	El impacto sobre la compañía es directo y medio, se podría incurrir en gastos operativos controlados, existen sanciones por falta leve, se expone la imagen de la Organización con un impacto medio. Afecta hasta en 24 horas las operaciones
2	Menor	Riesgo aceptable en el sector; no hay daño a la reputación, no hay sanciones legales, pero si observaciones por parte de los autoridades, el impacto operacional o financiero es mínimo. Afecta hasta en 6 horas las operaciones del instituto.
1	Insignificante	No hay impacto directo sobre la organización, no hay daño a la reputación, no existen sanciones legales ni impacto financiero u operacional. Tiene un efecto nulo o muy pequeño en las operaciones

Fuente: ISO/IEC 27005:2008

Una vez que se haya valorizado la probabilidad e impacto de cada uno de los riesgos detectados, se realizó una multiplicación entre estos valores para conocer el valor del riesgo, dependiendo del valor hallado se conoció el nivel del riesgo con la ayuda de la siguiente matriz de calor:

Tabla 4. 15 MATRIZ DE CALOR

IMPACTO						
	8	8	16	24	32	40
	6	6	12	18	24	30
	4	4	8	12	16	20
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		PROBABILIDAD				

Fuente: ISO/IEC 27005:2008

Se definió tres niveles de riesgo graficados en la matriz anterior, estas son:

- **Riesgos Bajos**: Aquellos riesgos cuyo valor oscila entre 1 y 8. Riesgos inferiores, deben ser tratados con los procedimientos de rutina ya definidos en la institución. Aquellos riesgos que no se encuentren en esta zona deberán ser tratados con ayuda de controles para minimizar su valor.
- **Riesgos Altos:** Aquellos riesgos cuyo valor oscila entre 9 y 18. Riesgos que deben ser tratados con procedimientos especiales con la ayuda de la implementación de algunos controles de seguridad, la Alta Dirección debe ser consciente de la existencia y tratamiento de estos riesgos.
- **Riesgos Graves**: Aquellos riesgos cuyo valor oscila entre 20 y 40. Riesgos que deben ser tratados de manera inmediata y con alta prioridad debido a lo que podría suceder si se materializa el riesgo, la Alta Dirección debe ser consciente de la existencia y tratamiento de estos riesgos.

Como se señaló previamente, el apetito de riesgo de la institución involucra aquellos riesgos cuya multiplicación de impacto y probabilidad oscila entre 1 y 8, es decir, solo los riesgos bajos, debido a ello, se recomendó monitorearlos para evitar que su probabilidad o impacto crezca en el tiempo.

Cualquier riesgo que exceda estos valores, debe ser tratado de manera inmediata para reducir su valor a un rango aceptable según lo indicado por la metodología de evaluación de riesgos.

A continuación se presenta la matriz completa de riesgos de los activos que entraron en el análisis, según el apetito de riesgo establecido.

Tabla 4. 16: Matriz de Riesgo

MATRIZ DE RIESGO									
Id riesgo	**Activo**	**Vulnerabilidad**	**Amenaza**	**Riesgo**	**Probabilidad**	**Impacto**	**Nivel de riesgo**	**Valor del riesgo**	**Tipo de tratamiento**
R1	Backup de Base de Datos Académico de Producción	-Errores al restaurar los backups. -Usuarios Inescrupulosos que se encuentran dentro o fuera del dominio.	-Se prueban los backups -Robo o destrucción de Backups de la Base de Datos	-Riesgo de pérdida de la integridad de la información almacenada en los backups debido a una restauración fallida de los mismos, a causa de la falta de pruebas de los backups. -Riesgo de pérdida o eliminación de los datos académicos vitales de los alumnos.	Bajo	Mayor	12	Riesgo Alto	Mitigar
R2	Historiales Académicos	-Pocos o nulos controles de Acceso -Falta de mecanismos de Backup	-Robo, pérdida o manipulación del Activo -Acceso nos autorizados al sistema. -Filtraciones de información	Riesgo de pérdida, daño o modificación de debido a robos o modificaciones no autorizadas, a causa de la falta de directivas y acuerdos de confidencialidad con personal externo y locadores	Bajo	Mayor	12	Riesgo Alto	Mitigar
R3	Certificados de Estudios	-Pocos o nulos controles de acceso -Falta de mecanismos	Robo, pérdida o manipulación del Activo.	Riesgo de pérdida, daño o modificación debido a robos o	Bajo	Mayor	12	Riesgo Alto	Mitigar

		de Backup.	-Acceso nos autorizados al sistema. -Filtraciones de información.	modificaciones no autorizadas, a causa de la falta de directivas y acuerdos de confidencialidad con el personal.					
R4	Informes Académicos	-Pocos o nulos controles de Acceso -Falta de mecanismos de Backup	Robo, pérdida o manipulación del Activo -Acceso nos autorizados al sistema -Filtraciones de información	Riesgo de pérdida, daño o modificación robos o modificaciones no autorizadas, a causa de la falta de directivas y acuerdos de confidencialidad con el personal.	Bajo	Mayor	12	Riesgo Alto	Mitigar
R5	Ficha de Datos personales del Estudiante	-Usuarios dentro o fuera del dominio realicen acciones ilícitas -Falta de cuidado en el transporte o en su transferencia	-Robo, pérdida o manipulación del Activo. -Acceso nos autorizados al sistema	Riesgo de pérdida, daño o modificación debido a robos o modificaciones no autorizadas, a causa de la falta de directivas y acuerdos de confidencialidad con el personal.	Bajo	Mayor	12	Riesgo Alto	Mitigar
R6	Ficha de Inscripción por cursos	-Usuarios dentro o fuera del dominio realicen acciones ilícitas -Falta de cuidado en el transporte o en su transferencia	Robo, pérdida o manipulación del Activo. -Acceso nos autorizados al sistema	Riesgo de pérdida, daño o modificación debido a robos o modificaciones no autorizadas, a causa de la falta de directivas y acuerdos de confidencialidad con el personal.	Bajo	Mayor	12	Riesgo Alto	Mitigar
R7	Datos de Actas	Usuarios dentro o	Manipulación	Robo de la	Moderado	Mayor	18	Riesgo	Mitigar

	Promocionales	fuera del dominio realicen acciones ilícitas	indebida en las actas promocionales de los Alumnos	información y manipulación maliciosa del sistema, por parte de personas sin autorización.				Alto	
R8	Datos de Notas Promocionales de Alumnos x Curso	Usuarios dentro o fuera del dominio realicen acciones ilícitas en la BD	Manipulación indebida de las Notas Promocionales de los Alumnos.	Robo de la información y manipulación maliciosa del sistema, por parte de personas sin autorización.	Moderado	Mayor	18	Riesgo Alto	Mitigar
R9	Reglamento Académico	Ambientes inseguro/inadecuado.	Deterioro Físico por condiciones ambientales Robo y mal uso de la información.	Robo de la información y manipulación maliciosa del sistema, por parte de personas sin autorización.	Bajo	Moderado	8	Riego Bajo	Se asume el riesgo
R10	Estatuto de la Universidad Nacional de Piura	Ambientes inseguro/inadecuado.	Robo y mal uso de la información Deterioro por antigüedad.	Robo de la información y manipulación maliciosa del sistema, por parte de personas sin autorización.	Bajo	Mayor	12	Riesgo Alto	Mitigar
R11	Manual de Usuario del Sistema Académico	Ambientes inseguro/inadecuado.	Robo y mal uso de la información Deterioro por antigüedad.	Riesgo de pérdida, daño debido a robos o accesos no autorizados, a causa de la falta de directivas y acuerdos de confidencialidad con el personal.	Bajo	Menor	4	Riesgo Bajo	Se asume el riesgo
R12	Actas de Notas	Usuarios dentro o fuera del dominio realicen acciones	-Acceso nos autorizados al sistema	Robo de la información y manipulación	Moderado	Mayor	18	Riesgo Alto	Mitigar

		ilícitas.	-Manipulación indebida de acta -Filtraciones de información.	maliciosa del sistema, por parte de personas sin autorización.					
R13	Boleta de Notas Académicas por alumno	Usuarios dentro o fuera del dominio realicen acciones ilícitas.	-Acceso nos autorizados al sistema -Manipulación indebida de boleta de notas -Filtraciones de información	Robo de la información y manipulación maliciosa del sistema, por parte de personas sin autorización.	Moderado	Mayor	18	Riesgo Alto	Mitigar
R14	Listado de Modificaciones autorizadas de notas	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Riesgo de pérdida, daño o modificación debido a robos o modificaciones no autorizadas, a causa de la falta de directivas y acuerdos de confidencialidad con el personal.	Bajo	Moderado	8	Riesgo Bajo	Se asume el riesgo
R15	Listado de Inscritos por cursos y secciones	Usuarios dentro o fuera del dominio realicen acciones ilícitas	Robo o manipulación del Activo	Riesgo de pérdida, daño o modificación debido a robos o modificaciones no autorizadas, a causa de la falta de directivas y acuerdos de confidencialidad con el personal.	Moderado	Moderado	12	Riesgo Alto	Mitigar
R16	Bitácora de acceso y cambios en las aplicaciones	Falta de bitácoras de acceso y cambios al Sistema.	Desconocimiento sobre los intentos y cambios de accesos y	Riesgo de modificación o pérdida de información, debido al desconocimiento sobre	Bajo	Mayor	12	Riesgo Alto	Mitigar

			acciones a la aplicación por parte de los usuarios	los intentos y cambios de acceso y aplicación. No se puede conocer con exactitud al personal que incumplió el procedimiento.					
R17	Base de Datos de Desarrollo	-Exceso de privilegios para usuarios no indicados -Usuarios Mal intencionados	-Falta de auditorías (supervisiones) programadas o Inopinadas -Falta de pruebas de hacking ético.	-Riesgo de compromiso de información debido a un ingreso no autorizado a la base de datos, a causa de la falta de auditorías a la base de datos -Riesgo de compromiso de información debido a ataques mal intencionados, causados por la falta de mecanismos de detección.	Bajo	Mayor	12	Riesgo Alto	Mitigar
R18	Backup de Base de Datos de Producción	-Falta de control y pruebas de seguridad de respaldo de Backus de la Base de Datos -Falta de ambiente de respaldo fuera instalaciones -Usuarios dentro o fuera del dominio realicen acciones	-Errores de manipulación al restaurar los backups -Robo o Destrucción del Backus de la Base de Datos.	-Riesgo de pérdida de la integridad de la información almacenada en los backups debido a una restauración fallida de los mismos, a causa de la falta de pruebas de los backups -Riesgo de pérdida o daño de la información	Bajo	Mayor	12	Riesgo Alto	Mitigar

		ilícitas		de los Backus debido a un evento que destruya el servidor por falta de políticas de respaldo de la información.					
R19	Backup de Base de Datos de Producción en Aplicativos Web	Puntos de acceso al sistema remotos a la red privada de la Empresa	Acceso de usuarios no autorizados a sistemas o Redes.	Riesgo de pérdida o daño de la información de los Backus debido a la obsolescencia en los controles de acceso a los aplicativos web.	Moderado	Mayor	18	Riesgo Alto	Mitigar
R20	Código Fuente Aplicativos Desktop	Usuarios mal intencionados que se encuentran dentro o fuera del dominio.	Modificación o Robo de Archivos de Código Fuente de Sistemas.	Riesgo de compromiso de información debido a ataques mal intencionados, causados por la falta de mecanismos de detección.	Bajo	Mayor	12	Riesgo Ato	Mitigar
R21	Claves cifradas de sistema informático	Usuarios malintencionados que se encuentran dentro o fuera del dominio.	Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas.	Robo de la información y manipulación maliciosa del sistema, por parte de personas sin autorización.	Bajo	Mayor	12	Riesgo Alto	Mitigar
R22	Contraseñas de empleados	Contraseñas de los usuarios sencillas.	Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas.	Robo de la información y manipulación maliciosa del sistema, por parte de personas sin autorización.	Bajo	Alto	12	Riesgo Alto	Mitigar
R23	Código Fuente de Aplicativos Web	Usuarios mal intencionados que se encuentran dentro o	Modificación o Robo de Archivos de	Riesgo de compromiso de información debido a ataques mal	Moderado	Mayor	18	Riesgo Alto	Mitigar

		fuera del dominio.	Código Fuente de aplicativos Web.	intencionados, causados por la falta de mecanismos de detección.					
R24	CD de Backup de Producción	-Almacenamiento del Backup dentro del área. -Poca higiene en el lugar donde se guarda las cintas.	-Desastre Natural -Deterioro permanente de las CD.	Riesgo de pérdida o deterioro de los CD's con los backups de la información del área debido a un desastre natural , a causa de su almacenamiento dentro de la misma área	Bajo	Mayor	12	Riesgo Alto	Mitigar
R25	Herramientas de Desarrollo	Descarga de Herramientas sin Licencia desde el Internet.	-Inestabilidad en las aplicaciones desarrolladas. -Uso de software ilegal.	-Riesgo de denuncia por problemas legales de licenciamiento. -Riesgo de afección por malware generando inestabilidad en las aplicaciones y red local. - Riesgo de perder la certificación de calidad ISO. -Riesgo de no poder descargar las últimas actualizaciones, quedando obsoleto el programa, generando inestabilidad y hoyos de seguridad.	Moderado	Moderado	12	Riesgo Alto	Mitigar

R26	Licencia SQL Server	-Mala gestión de contraseñas -Falta de mecanismos de autenticación e identificación de usuarios	-Abuso o forzado de derechos -Uso de software ilegal.	-Riesgo de denuncia por problemas legales de licenciamiento. -Riesgo de afección por malware generando inestabilidad en las aplicaciones y red local. - Riesgo de perder la certificación de calidad ISO. -Riesgo de no poder descargar las últimas actualizaciones, quedando obsoleto el programa, generando inestabilidad y hoyos de seguridad.	Moderado	Moderado	12	Riesgo Alto	Mitigar
R27	Licencia .Net	-Mala gestión de contraseñas -Falta de mecanismos de autenticación e identificación de usuarios	-Abuso o forzado de derechos -Uso de software ilegal.	-Riesgo de denuncia por problemas legales de licenciamiento. -Riesgo de afección por malware generando inestabilidad en las aplicaciones y red local. - Riesgo de perder la certificación de calidad ISO. -Riesgo de no poder descargar las últimas	Bajo	Mayor	12	Riesgo Alto	Mitigar

				actualizaciones, quedando obsoleto el programa, generando inestabilidad y hoyos de seguridad.					
R28	Sistema Operativo de Servidor Windows Server 2013	-Presencia de Virus o Código Malicioso o personal no autorizado (Hackers).	Daño del Sistema operativo. Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada.	Pérdida o daño a la información o al sistema que maneja los recursos y materiales que se usan, por parte de hackers.	Bajo	Mayor	12	Riesgo Alto	Mitigar
R29	ANTIVIRUS ESET ENDPOINT SECURITY	-Presencia de virus o código malicioso.	Sistema de Protección Desactualizado y desfasado o No licenciado	Pérdida o daño a la información o al sistema que maneja los recursos y materiales que se usan,	Bajo	Mayor	12	Riesgo Alto	Mitigar
R30	Servidor de Aplicaciones Web	-Personas dentro o fuera del dominio accedan y manipulen indebidamente los equipos. -Acceso no Autorizado de Personas Ajenas a las Instalaciones. -Falta de una adecuada gestión de reemplazo o mantenimiento.	-Acceso y operación de equipos remotamente sin autorización - Manipulación, Robo. - Destrucción de equipos o medios de comunicación.	-Riesgo de compromiso de información debido a ataques mal intencionados, causados por la falta de mecanismos de detección. Riesgo de daño o deterioro del servidor debido a un mantenimiento insuficiente, a causa del incumplimiento del plan de mantenimiento	Moderado	Mayor	18	Riesgo Alto	Mitigar

				.					
R31	Servidor de Aplicaciones Desktop	-Personas dentro o fuera del dominio accedan y manipulen indebidamente los equipos. -Acceso no Autorizado de Personas Ajenas a las Instalaciones. -Falta de una adecuada gestión de reemplazo o mantenimiento.	-Acceso y operación de equipos remotamente sin autorización - Manipulación, Robo. - Destrucción o daño de equipos o medios de comunicación.	- Riesgo de compromiso de información debido a ataques mal intencionados, causados por la falta de mecanismos de detección. - Riesgo de daño o deterioro del servidor debido a un mantenimiento insuficiente, a causa del incumplimiento del plan de mantenimiento.	Moderado	Mayor	18	Riesgo Alto	Mitigar
R32	PC de Desarrollo	-Mala seguridad de Contraseñas. -Falta concientización del usuario. -Sensibilidad a la humedad, polvo y al calor - Continúa presencia de Interrupciones de Fluido Eléctrico -Perdida de conexión a la red, interna e internet, debido a la falla del equipo.	-Manipulación del Activo - Filtraciones de información y accesos no autorizados - Deterioro y daño por polvo, corrosión. -Falla del equipo de telecomunicacio-nes.	-Riesgo de pérdida o daño de la información debido A la debilidad de contraseñas. -Riesgo de pérdida de la información debido al acceso no autorizado de usuarios. -Riesgo de daño o deterioro de los equipos del debido al polvo a factores ambientales, a causa de la falta de mecanismos para controlar el medio	Moderado	Moderado	12	Riesgo Alto	Mitigar

				ambiente					
R33	DataCenter	-Protección física inapropiada para el centro de procesamiento de datos -Poco personal capacitado en el uso de extintores. Falta de mecanismos para el respaldo de información -Susceptibilidad a la humedad, el polvo y la suciedad. -UPS tiene una duración máxima de 30 minutos - Niveles de seguridad perimetral débiles o poco confiables - Falta de mecanismos tecnológicos adecuados para control de acceso	-Destrucción de equipo o medios -Fuego -Deterioro por polvo, corrosión, congelamiento. -Pérdida del suministro de energía. -Acceso no autorizado.	-Riesgo de compromiso de los activos almacenados en el DataCenter debido a algún acto mal intencionado, causado por la falta de una protección física que evite estos actos -Riesgo de daño o deterioro de los equipos del DataCenter debido al polvo a factores ambientales, a causa de la falta de mecanismos para controlar el medio ambiente -Riesgo de pérdida de disponibilidad de los equipos almacenados en el DataCenter debido a la falta de energía Eléctrica, causados por la poca duración de los UPS adquiridos.	Moderado	Catastrófica	24	Riesgo Grave	Eliminar
R34	Diseño de infraestructura de red	Personas dentro o fuera del dominio con Intensiones de espionaje	Robo o Pérdida del Diseño de la Infraestructura de Red	Riesgo de daño o pérdida del diseño de infraestructura de la red por terceros	Bajo	Menor	4	Riesgo Bajo	Se asume el riesgo
R35	Switch,	-Robo o	Problemas de	Riesgo de pérdida de	Moderado	Moderado	12	Riesgo	Mitigar

	Enrutadores, Conmutadores de red	manipulación de equipos - Perdida de conexión a la red, interna e internet, debido a la falla del equipo	Red de Datos.	disponibilidad de los equipos y sistemas.				Alto	
R36	Fuentes de alimentación	Mantenimiento insuficiente.	-Incumplimiento en el mantenimiento del sistema -Antigüedad del equipo.	- Riesgo de deterioro o pérdida del equipo o equipos conectados a este.	Bajo	Mayor	12	Riesgo Alto	Mitigar
R37	Sistemas de alimentación ininterrumpida	-Mantenimiento insuficiente -El funcionamiento del DataCenter depende de los UPS.	-Incumplimiento en el mantenimiento del sistema. - Antigüedad del equipo.	Riesgo de deterioro de los equipos UPS debido a fallas del equipo, a causa de la falta de mantenimiento. - Riesgo de deterioro de los equipos UPS debido a fallas del equipo, a causa de su antigüedad	Moderado	Mayor	18	Riesgo Alto	Mitigar
R38	Sistemas contra incendios	Equipos de detección Defectuosos o mal Calibrados.	Fallas de detección e inoperatividad del Sistema.	Riesgo de deterioro del equipo debido a fallas, a causa de la falta de mantenimiento. - Riesgo de deterioro debido a fallas del equipo, a causa de su antigüedad.	Moderado	Moderado	12	Riesgo Alto	Mitigar
R39	Sistemas de aire acondicionado	Cortes de Fluido Eléctrico.	Deterioro de Equipos de Enfriamiento.	Riesgo de deterioro del equipo debido a fallas, a causa de la falta de	Moderado	Moderado	12	Riesgo Alto	Mitigar

	-			mantenimiento. - Riesgo de deterioro debido a fallas del equipo, a causa de su antigüedad					
R40	Sistemas de filtrado de aire	Falta de mantenimiento.	Deterioro de equipos.	Riesgo de deterioro del equipo debido a fallas, a causa de la falta de mantenimiento. - Riesgo de deterioro debido a fallas del equipo, a causa de su antigüedad	Moderado	Moderado	12	Riesgo Alto	Mitigar
R41	Identificadores biométricos de los empleados	Falta de mantenimiento.	Fallas de detección e inoperatividad.	Riesgo de deterioro del equipo debido a fallas, a causa de la falta de mantenimiento. - Riesgo de deterioro debido a fallas del equipo, a causa de su antigüedad	Moderado	Moderado	12	Riesgo Alto	Mitigar
R42	Correo electrónico	-Falta de concientización -Acceso por parte de terceros. -Correos electrónicos Spam, Hoax.	-Suplantación de identidad. -Espionaje -Infidencia/Fuga de Información. - Pueden contener virus, Troyanos o archivos maliciosos.	-Riesgo de pérdida o daño de la información de los correos recibidos debido a la falta de capacitación de seguridad en el área -Divulgación de información confidencial de la empresa mediante el correo electrónico, por parte del personal del área	Moderado	Moderado	12	Riesgo Alto	Mitigar

R43	Microsoft Outlook® Web Access (OWA)	Problemas Técnicos con Servidores de Correo.	Indisponibilidad del Servicio.	-Riesgo de pérdida o daño de la información de los correos recibidos debido a la falta de un plan de mantenimiento del servidor y de capacitación de seguridad en el área -Divulgación de información confidencial de la empresa mediante el correo electrónico, por parte del personal del área	Moderado	Moderado	12	Riesgo Alto	Mitigar
R44	Microsoft Active Directory®	Deficientes políticas de autenticación y validación de Acceso.	Acceso de Personas no autorizadas a los recursos de red.	Riesgo de pérdida o daño de la información de personas no autorizadas a la red.	Moderado	Moderado	12	Riesgo Alto	Mitigar
R45	Sistema de nombres de dominio (DNS)	Problemas de Hardware o desconfiguración por presencia de Virus.	Inoperatividad del Servicio de asignación dinámica de Nombres	Riesgo de disponibilidad del servicio.	Moderado	Moderado	12	Riesgo Alto	Mitigar
R46	Protocolo de configuración dinámica de host (DHCP)	Problemas de Hardware o Desconfiguración por presencia de virus.	Inoperatividad del Servicio de asignación dinámica de Direcciones IP.	Riesgo de disponibilidad del servicio.	Moderado	Moderado	12	Riesgo Alto	Mitigar
R47	Uso compartido de Recursos (Impresoras,	-Mantenimiento insuficiente. -Inactividad del equipo debido a la	-Incumplimiento en el mantenimiento de la herramienta	-Riesgo de daño o deterioro de las impresoras. comunes debido a un	Moderado	Menor	6	Riesgo Bajo	Se asume el riesgo

	fax, etc.)	falta de energía	-Perdida del suministro de energía	mantenimiento insuficiente, a causa del incumplimiento en el mantenimiento rutinario. -Riesgo de pérdida de disponibilidad de las impresoras comunes debido a la pérdida de Energía.					
R48	Acceso a red privada virtual (VPN)	Problemas Técnicos de Hardware o Software.	Inaccesibilidad.	Riesgo de disponibilidad y acceso no autorizados a la red	Bajo	Mayor	12	Riesgo Alto	Mitigar
R49	Dispositivo firewall de hardware y software	Problemas Técnicos de Hardware o Software	Inaccesibilidad.	Riesgo de personas autorizadas a la red. -Riesgo de robo de información por virus o hacker. -Riesgo de daño del equipo debido a una falta de un plan de mantenimiento.	Moderado	Mayor	18	Riesgo Alto	Mitigar
R50	Cableado de red	Problemas con algún punto de la red.	No existe un rotulado del cableado estructural	Riesgo de problemas en la infraestructura de red debido a problemas de conexión en el cableado, a causa de la falta de un rotulado adecuado	Moderada	Mayor	18	Riesgo Alto	Mitigar
R51	Fibra Óptica	Falla del proveedor	Caída del Servicio	Riesgo de problemas en la infraestructura de	Bajo	Catastrófica	12	Riesgo Alto	Eliminar

				red debido a problemas naturales o faltas de mantenimiento.					
R52	PC de oficina	-Inactividad del equipo debido a la falta de energía -Mantenimiento insuficiente -Falta de políticas para el respaldo de información -Falta de actualización de antivirus	-Pérdida del suministro de energía -Incumplimiento en el mantenimiento de equipo. -Destrucción del equipo o los medios. -Introducción de virus, troyanos o software malicioso	-Riesgo de pérdida del acceso a la información del Sistema. -Riesgo de pérdida de disponibilidad de las aplicaciones. -Riesgo de daño o deterioro de las computadoras debido a un mantenimiento insuficiente, a causa del incumplimiento en el mantenimiento rutinario -Riesgo de pérdida de la información almacenada en la computadora debido a algún evento que destruya el equipo, a causa de la falta de políticas para el respaldo de información. -Riesgo de pérdida o daño de la información o de deterioro de la computadora debido a	Moderado	Mayor	18	Riesgo Alto	Mitigar

				un ataque mal intencionado, a causa de la falta de un software para el tratamiento de código malicioso					

Fuente: ISO/IEC 27005(2008)

4.7. CONTROLES PARA EL TRATAMIENTO DE LOS RIESGOS

4.7.1. Declaración de Aplicabilidad

Los controles que se han seleccionado para el tratamiento de los riesgos son los que se detallan en el estándar ISO/IEC 27001, el cual contiene una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones en general. Cabe resaltar que dichos controles siguen lineamientos generales, en la Declaración de la Aplicabilidad se mostrarán los controles adaptados a la realidad institucional de la Universidad Nacional de Piura

Para empezar se definió controles respecto a las políticas de seguridad que la institución busca establecer para alcanzar el nivel de seguridad deseado. Cabe resaltar que todos estos controles o políticas contribuyen a la mitigación de todos los riesgos identificados y, en su mayoría, deberán ser desarrollados y promovidos por las autoridades de la institución.

Estos controles y políticas de seguridad son los siguientes:

Tabla 4. 17:DECLARACIÓN DE APLICABLIDAD

CONTROLES PROPUESTOS

5 .POLITICAS DE SEGURIDAD DE LA INFORMACIÓN			
OBJETIVOS DE CONTROL	CONTROL	APLICABILIDAD	DESCRIPCION
5.1 DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD DE LA INFORMACIÓN.	5.1.1.Políticas para la Seguridad de la Información.	APLICAR	-Establecer y publicar una Política General de Seguridad de la información y comunicar a todos los niveles, empleados y terceras partes que lo requieran. Y en caso sea pertinente, políticas específicas para cada uno de los casos que así lo requieran por ejemplo: - Política del buen uso de los recursos institucionales. - Política del buen uso del internet - Política del buen uso del correo institucional. -En la implementación , se debe considerar la inclusión de los siguientes aspectos: - Desarrollar Marco general para la gestión y evaluación de riesgos. - Establecer lineamientos para el cumplimiento de las normas internas y requerimientos de contratos. - Establecer los requerimientos de educación y entrenamiento de seguridad de información. - Establecer sanciones de las violaciones de la política de seguridad. - Definir responsabilidades de la administración de seguridad de información.(responsables y roles)

	5.1.2.Revisión de las Politicas para la Seguridad de la Información	APLICAR	Se sugiere establecer un lineamiento (o política) que norme la revisión periódica de las políticas de seguridad (idealmente cada año) para asegurar el cumplimiento de las modificaciones o nuevas normas legales que involucren a la institución, así como los cambios internos que pueda sufrir. Para ello se sugiere implementar un procedimiento considere los siguientes directrices: - Revisión de controles implementados. - Sugerencia de mejora a estos controles. - Acciones correctivas y preventivas. - Verificación del cumplimiento de políticas de seguridad. - Sugerencias de mejora de la organización de seguridad. - Reportes de incidentes de seguridad de información. - Recomendaciones proporcionadas por los involucrados.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			
6.1 ORGANIZACIÓN INTERNA	6.1.1.Asignación de Responsabilidades para la Seguridad de la Información.	APLICAR	- Asignar y documentar todas las responsabilidades sobre la seguridad de información por cada uno de los activos y procesos de seguridad. - Definir y documentar los niveles de autoridad. Para ello se sugiere implementar : - Un comité de seguridad de la información así también designar al oficial de seguridad, fuertemente apoyada por las autoridades y que cubra todos los objetivos de seguridad de información de acuerdo a la política de seguridad de información. - El Comité de Seguridad de Información, debe

			estar conformado por los decanos de cada facultad y el personal designado por cada área del CIT y OCRA, quienes trabajarán en coordinación constante con el Oficial o Coordinador de Seguridad de Información, quién a su vez, debe liderar las reuniones proponiendo temas relativos a la implementación de nuevos controles de seguridad de información y organizar la participación de los otros miembros del comité.
	6.1.2 Segregacion de tareas	APLICAR	Especificar y documentar la separación de funciones .
	6.1.3.Contacto con las autoridades	APLICADO	Se mantiene contacto con autoridades.
	A 6.1.4 Contacto con grupos de interés especial	APLICAR	Se debe mantener contactos con grupos de interés especial u otros foros de especialistas relacionados en seguridad de la información así como de asociaciones profesionales mediante los cuales se pueda actualizar conocimientos sobre aspectos de seguridad de información; recibir en forma oportuna consejos, alertas y parches frente ataques y vulnerabilidades; compartir e intercambiar información acerca de tecnologías, productos, amenazas o vulnerabilidades; Se sugiere tener contacto con la ONGEI, encargada de supervisar la implementación del SGSI a nivel nacional.
	A 6.1.5 Seguridad de la información en la gestión de proyectos.	APLICADO	Utilizan una metodología de gestión de proyectos.
6.2 DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO	A 6.2.1 Política de uso de dispositivos para movilidad	APLICAR	Desarrollar e implementar una política restringe la conexión a las redes inalámbricas de internet por parte de los dispositivos móviles y equipos de terceros.

	A 6.2.2 Teletrabajo	NO APLICADO	NO SE CONSIDERA DADO QUE NO SE TIENE EL SERVICIO DE TELETRABO EN LA INSTITUCION.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			
7.1 ANTES DE LA CONTRACION	A 7.1.1 Investigacion de Antecedentes	APLICADO	Como parte del proceso de selección y reclutamiento se revisan los antecedentes Penales y policiales de cada uno de los candidatos a un puesto laboral.
	A 7.1.2 Términos y condiciones del empleo	APLICAR	Establecer un procedimiento donde se especifique que antes del inicio de un empleo firma del contrato, debe contener los siguiente: - Considerar políticas de seguridad de información de la institución. - Definir con claridad los roles y responsabilidades del personal que ejecutará el servicio. - Definir con claridad los activos asignados al personal y la protección de los mismos. - Establecer un documento sobre la confiabilidad de la información y activos asignados. - Definir con claridad las sanciones a las violaciones de las políticas de la institución. - Código de Ética y de Conducta. - Procedimientos de seguridad. - Reglamento de seguridad y salud en el trabajo. - Política de uso de correo electrónico. - Reportes de incidentes y riesgos contra la seguridad de información.
7.2 DURANTE LA CONTRACION	.7.2.1. Responsabilidades de gestión.	APLICAR	Las autoridades deben desempeñar las siguientes funciones: − Participar activamente en la difusión de la política de seguridad de información. − Informar sobre los roles y responsabilidades en materia de seguridad de información antes de otorgar acceso a información sensible o a los

			sistemas de información. - Proveer las pautas del nivel de seguridad de información que espera dentro del desempeño de sus funciones. - Asegurarse que los usuarios alcancen el nivel de conocimiento suficiente en materia de seguridad, para el desempeño óptimo de sus roles y responsabilidades.
	7.2.2. Concienciación, educación y capacitación en seguridad de la información.	APLICAR	-Establecer un plan de entrenamiento o capacitación que se inicie con la inducción y que introduzca conocimiento de las políticas de seguridad de la institución antes que los servicios o información se ponga a disposición del empleado, contratistas o terceras partes. Para ello se realizará anualmente y que además, considere los siguientes aspectos: - Requerimiento de seguridad. - Actualizaciones de los procesos y políticas. - Responsabilidades legales. - Controles de la institución.
	7.2.3. Proceso disciplinario.	APLICAR	Implementar un procedimiento para la ejecución de procesos disciplinarios en el caso de constatar que se ha cometido una violación a las políticas de seguridad., se seguirá las siguientes directrices: - Deterninar la naturaleza y gravedad de la violación de la seguridad y el impacto sobre el negocio. - Verificar si el infractor ha sido o no adecuadamente entrenado en materia de seguridad de información. - Si ha sido entrenado, verificar si es primera

			vez o se ha efectuado repetidas veces. − En caso de ser una violación grave, se debe retirar los derechos y privilegios de acceso y, de ser necesario, retirar al infractor inmediatamente de su ambiente de trabajo. − Realizar las sanciones correspondientes. − Si no ha sido entrenado, verificar si es primera vez o se ha efectuado repetidas veces. − En ambos casos, realizar las medidas correspondientes de acuerdo a la gravedad e impacto del mismo. -Difundir periódicamente a todo el personal respecto a los procesos disciplinarios implementados, con el propósito de crear conciencia sobre el cumplimiento de las políticas de seguridad.
7.3 CESE O CAMBIO DE PUESTO DE TRABAJO	7.3.1 Cese o cambio de puesto de trabajo.	APLICAR	- Implementar un procedimiento mediante el cual se proceda a poner fin a las responsabilidades relacionadas a un servicio, que estuvo sujeto al momento de su incorporación a la institución. El cual es el siguiente: − Generar un listado de activos asignados. − Realizar la verificación fisica de los activos asignados, registra el resultado y realiza las observaciones del caso: (Faltante, deteriorado, etc). − Restringuir el acceso a los sistemas de información, correo institucional y otros. − Reportar la información a la instancia correspondiente. − Si existen diferencias informar a través de un correo y documento a la instancia

			correspondiente la existencia faltante de activos. − Realizar las medidas correspondientes según lo detectado como resultado del inventario, el cual puede ser perdida, robo, ubicado en otro lugar ,etc. - Los cambios de responsabilidad o empleo (dentro de la misma institución), deben ser tratados como una finalización de responsabilidades, y la nueva responsabilidad o empleo deben tratarse con controles "antes de la contratación" (acápite 7.1)
8. GESTION DE ACTIVOS			
8.1 Responsabilidad sobre los activos.	8.1.1 Inventario de activos.	APLICAR	La Institución tiene un inventario de activos. Sin embargo se sugiere clasificar de acuerdo a su sensibilidad y criticidad, para tener un control permanente de los mas representativos para la institución. Para lo cual se mencionan algunas directrices: - Tener en cuenta el análisis realizado de criticidad Alto, Bajo, Medio. - Rotular los activos de acuerdo a la clasificación sugerida. - Asignar un propietario y las responsabilidades de los controles de mantenimiento a dicho activo. - Mostrar detalles importantes de los activos para su gestión como : Ubicación, Area, Tipo de Activo, Número de Serie, Número de versión,estado, etc. - Incluir el uso de códigos de barras para facilitar las tareas de realización de inventario y para vincular equipos de TI que entran y salen de las instalaciones con empleados. - Para incluir o modificar un activo, el

			propietario enviará una solicitud para incluir o modificar el activo de información a través del correo institucional, estableciendo Nombre del activo, Tipo de activo y la valoración de la - confidencialidad, integridad y disponibilidad. (Ver Clasificación de Activos del Análisis realizado.) - El oficial de Seguridad de la Información o quien haga sus veces realizará la validación de inclsuión o modificación de la solicitud, enviando un correco al solicitante, notificando el resultado de la validación. - Revisar anualmente el invetario, con el fin de ajustar la programación para el próximo año.Teniendo en base los criterios establecidos. - Adquirir una herramienta ya sea gratuita o licencia de gestión de activos. Para lo cual se propone: - Genos Open Source(Gratuita). - GesConsultor(Licenciada).
	8.1.2 Propiedad de los activos.	APLICAR	Se firman documentos , donde se detalla la asignación y responsable del activo. Este documento debe contener: - Nombre del activo. - Tipo de Activo. - Propietario. - Código de barras para su identificación. - Ubicación(Área, proceso, etc).
	8.1.3 Uso aceptable de los activos.	APLICAR	- Especificar y documentar las reglas para el uso aceptable de la información y los activos de la institución mediante una política o procedimiento que debe ser conocido por el personal del área. - Algunas directrices a tener en cuenta para las

			estaciones de trabajo son las siguientes: - Todas las estaciones de trabajo deben tener usuario y contraseña asociados a un empleado. - No divulgar contraseña, usuario o datos importantes. - Uso de software antivirus provisto por el Area de Soporte. - Restricción de privilegios de acuerdo a su perfil. - Uso de software licenciado. - Realizacion de copias de seguridad - Permanecer siempre cerca al dispositivo. - No dejar desantendidos los equipos a excepción de alguras tareas propias de sus funciones. - Sesiones cerradas cuando haya pasado 10 minutos de inactividad. - No conectarse a rede wifi.
	8.1.4 Devolución de activos.	APLICAR	-Actualmente, la institución tiene un formato para la devolución de equipos asignados; sin embargo se debe establecer un procedimiento detallado para la devolución de activos en toda la institución. Ejemplo: - Software(manuales de software,etc) - Documentos institucionales - Equipos informáticos. - Sofware e Información guardada en medios extraíbles. -En casos donde un trabajador tiene conocimiento que es importante para las operaciones o actividades, está debe ser documentada y transferida a la institución. -Se deberá generar un comunicado al CIT para que

			procedan a bloquear todos los accesos del usuario y pasarlo a estado inactivo.
8.2 Clasificación de la información.	8.2.1 Directrices de clasificación.	APLICAR	- Realizar la clasificación de activos de acuerdo a su confidencialidad y criticidad. La institución debe asegurar que la información reciba un nivel apropiado de protección, así mismo todos los usuarios deben de estar comprometidos en respetar la clasificación de la información propuesta o definida. - La clasificación debe ser realizada con la ayuda del propietario de la información para indicar si la información es critica, confidencial o de otra índole.
	8.2.2 Etiquetado y manipulado de la información.	APLICAR	Desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la institución. Toda información que sea clasifica como "confidencial" debe de poseer una etiqueta de seguridad que provea todos los datos correspondientes a esta categoría.
	8.2.3 Manipulación de activos.	APLICAR	Desarrollar e implementar procedimientos para la manipulación de activos, de acuerdo con el esquema de clasificación de información adoptado por la institución. En el procedimiento se sugiere incluir: - Bitácoras de fallas detectadas en los equipos. - Definir y documentar el uso adecuado y tratamiento de los activos.
8.3 Manejo de los soportes de almacenamiento.	8.3.1 Gestión de soportes extraíbles.	APLICAR	- Implementar procedimientos para la gestión de medios extraíbles, de acuerdo con el esquema de clasificación adoptado por la institución - Establecer un formato de asignación de propietario de medios removibles tales como,

			correo electrónico laboral, servicios de mensajería, USB, CD, entre otros además de un formato para la entrega o custodia y destrucción de tales medios o dispositivos.
	8.3.2 Eliminación de soportes.	APLICAR	La eliminación de soporte que contiene información confidencial debe seguir un protocolo que asegure su correcto desecho, de manera que no pueda ser reutilizado por otras personas no autorizadas.
	8.3.3 Soportes físicos en tránsito.	APLICAR	-Se debe llevar a cabo un procedimiento en el manejo y almacenamiento de la información, para asegurar la que se eviten eventos como divulgación, modificación, retiro o destrucción de información no autorizada cuando se traslade un medio físico de un punto a otro.
9. CONTROL DE ACCESOS.			
9.1 Requisitos de negocio para el control de accesos.	9.1.1 Política de control de accesos.	APLICAR	-La institución día a día genera y desarrolla activos de información lo cuales deben estar salvaguardados o custodiados de acuerdo a su importancia o clasificación por lo que se debe controlar el acceso a la información. Por lo tanto se debe: - Desarrollar e implementar una política de control de acceso, documentada, revisada y basada en los requerimientos de seguridad y objetivos institucionales. - Implementar controles adicionales a los que se cuenta actualmente considerando los siguientes directrices: - Definir y documentar accesos a sistemas de informacion, recursos, servicios y redes de comunicacion de acuerdo a la naturaleza del usuario y roles existentes dentro de la institución. - Controlar los accesos de acuerdo a los perfiles y privilegios existenes en los sistemas.

			- Implementar políticas para la difusión y autorización de la información. Se requiere conocer los principios y niveles de seguridad, y la clasificación de la información.
			
			  - Desarrollar procedimiento para la autorización formal de solicitudes de acceso.
			  - Desarrollar procedimiento para la revisión periódica de los controles de acceso.
			  - Los responsables de la asignacion y autorizacion de acceso comunicarán las politicas y monitorearan el cumplimiento de estos.
			- Identificar toda la información relacionada a las aplicaciones de la institución y los riesgos a las que están expuesta (análisis de riesgo de la información de las aplicaciones).

	9.1.2 Control de acceso a las redes y servicios asociados.	APLICAR	Implementar una política concerniente al uso de redes y servicios de red. Esta debe comprender: - Las redes y servicios de red a los cuales se permite el acceso. - Procedimientos de autorización para determinar las personas que tienen permitido el acceso a las redes y los servicios de red. - Controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red. - Los medios utilizados para acceder la red y los servicios de red (condiciones para disponer de servicios Internet o uso de equipos remotos).

9.2 Gestión de acceso de usuario.	9.2.1 Gestión de altas/bajas en el registro de usuarios.
	.
		APLICAR	La institución está aplicando este control. Sin embargo se deberá implementar las siguientes directrices para mejorar el control actual.
			- Implementar un procedimiento formal por escrito de alta del usuario al sistema, que regule y exija el ingreso de los siguientes datos:
			  - Usuario.
			  - Tipo o nivel de usuario al que pertenece.
			  - Password(requerimientos mínimos)
			  - Nombre y apellidos completo
			  - Contador de intentos fallidos
			  - Permisos mínimos y necesarios de acuerdo a su nivel o tipode usuario para que desempeñe su tarea.
			- Implementar un procedimiento formal por escrito de baja de usuario al sistema, teniendo en cuenta lo siguiente:
			  - Fecha de anulación
			  - Estado inactivo

	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	APLICAR	Implementar controles adicionales a los que se cuentan actualmente, incluyendo:
			- EL jefe de CIT deberá establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios.
			- Ristringuir el acceso a los sistemas o la utilización de recursos en un horario definido, teniendo en cuenta que:
			  - Las cuentas de los usuarios no deben poder acceder al sistema en horarios no laboral, de acuerdo al tipo o clasificación que pertenezcan.
			  - Durante las vacaciones o licencias las cuentas de los usuarios deben desactivarse
			  - En los días feriados las cuentas de los

			usuarios, a excepción de aquellos que lo requieran, deben permanecer desactivadas.
	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	APLICAR	Tomar en consideración los siguiente controles para mejorar el nivel de seguridad actual : – Identificar y documentar los privilegios asociados a cada producto del sistema (sistema operativo, sistema de administración de bases de datos y aplicaciones), y las categorías de personal a las cuales deben asignarse los productos. - Se debe mantener un procedimiento de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización. - Las autorizaciones de privilegios especiales de derechos de acceso deben revisarse a intervalos más frecuentes (se recomienda un periodo de tres meses). - El administrador del Sistema y Base de Datos debe poder loguearse solamente dentro de la institución y en una terminal especifica y hablitada por la misma.
	9.2.4 Gestión de información confidencial de autenticación de usuarios.	APLICAR	Implementar controles adicionales a los que se cuentan actualmente, incluyendo: -Establecer lineamientos para la autenticación e identificación de usuarios considerando los siguientes aspectos: - Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos)

			deben tener un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable - Se sugiere que ante la ausencia del personal por permisos, vacaciones, etc. se suspenda temporalmente la cuenta de dicho usuario, hasta su reincorporación a sus labores. Para el caso específico de la comunicación vía mail, se sugiere programar una respuesta automática que informe sobre el motivo de la ausencia de la persona y a la vez comunicar los datos de la persona que reemplazará a la ausente.
	9.2.5 Revisión de los derechos de acceso de los usuarios	APLICAR	Relizar a cabo una revisión periódica (se recomienda semestralmente) y después de cualquier cambio, como promoción o finalización de empleo para asegurar que cada usuario solamente tenga acceso a la información que requiere para sus funciones.
	9.2.6 Retirada o adaptación de los derechos de acceso	APLICAR	Desarrollar e implementar una política donde se exija el retiro de todos los derechos de acceso al empleado o tercero, que deje de laborar en la institución. El procedimiento debe considerar no sólo la baja de usuarios en el sistema sino también el retiro de los derechos de acceso accesos físicos y lógicos, tales como claves para ingresos a las instalaciones (en el caso de disponer de un dispositivo de control de acceso), fotochecks, entre otros.
9.3 Responsabilidades del usuario.	9.3.1 Uso de información confidencial para la autenticación	APLICAR	Se debería exigir y promover a los usuarios que cumplan las buenas prácticas de la institución para el uso de información de autenticación. Para lo cual se deberá hacer firmar al usuario un documento sobre la

			confiabilidad de la información que tiene acceso y las sanciones si infringe dicho control.
9.4 Control de acceso a sistemas y aplicaciones.	9.4.1 Restricción del acceso a la información.	APLICAR	- Desactivar las sesiones tras un período definido de inactividad o establecida cuando se finalizó los plazos dados por calendario académico. - Dar acceso a la información y a las funciones del sistema de aplicaciones solo a los usuarios de éste, incluido el personal de apoyo de acuerdo con una política de control de accesos definida.
	9.4.2 Procedimientos seguros de inicio de sesión.	APLICAR	-La institución ha implementado procedimientos básico de inicio de sesión. Si embargo se debe incluir las siguientes directrices para mejora el nivel de seguridad: -Implementar un política de control de accesos para controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-in. Los cuales se incluirán a los que actualemte tiene la isntitución. Estos son: – Tarjeta de coodenadas o Biometricos de identificación. – Bloqueo del usuario al intento fallidos de tres veces al sistema. El sistema registrará : la fecha y hora, el usuario, la terminal(Dirección IP). Estos se comunicarán al Administrador del Sistema para las medidas respectivas.
	9.4.3 Gestión de contraseñas de usuario.	APLICAR	-Se sugiere incluir los siguientes controles para mejorar las políticas y procedimientos implementados: Se mencionan algunas directrices para la gestión de contraseñas: – Realizar una evaluación a los sistemas de

			gestión de contraseñas, ya que estas deberían ser seguras y asegurar la calidad de las contraseñas. - Promover el protocolo de las buenas prácticas de la creación de una contraseña por parte de los usuarios. - No usar el mismo password para la institución y para asuntos personales. - Evitar reutilizar o reciclar antiguas contraseña. - No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar. - No habilitar la opción recordar clave en este equipo“, que ofrecen los programas - No enviarla por correo electrónico - Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc - Establecer el cambio de clave periódicamente, por consiguiente la existencia de una Política del buen uso de las contraseñas, y que su prestación o mal uso se considere falta grave. - Firmar una declaración por la cual se comprometen a mantener los password personales en secreto (esto podría incluirse en los términos y condiciones de empleo). -Directrices para creación de una contraseña segura: - Utilizar como mínimo 8 caracteres. - Uitlizar como mínimo un símbolo. - Utilizar mayúsculas y minusuclas. - Construir la contraseña a través de una frase fácil de recordar. - No utilizar información personal fácil de conseguir. - Nunca utilizar palabras del diccionario. - Nunca utilizar nombres comunes en

			informática(admin, root, etc)
	9.4.4 Uso de herramientas de administración de sistemas.	APLICAR	- Es necesario realizar un procedimiento documentado, en el cual se indique que cada jefe de área, debe solicitar los permisos adecuados para cada personal que se le autorice. - Restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.

	9.4.5 Control de acceso al código fuente de los programas	APLICAR	Implementar a los controles ya establecidos:
			- Un política o procedimiento documentado de acceso al código fuente de los sistemas informáticos. Esta debe comprender:
			  - Un registro de personas autorizadas y funciones.
			  - La fecha de ingreso y salida.
			  - El motivo de acceso.
			- Los programadores no podrán acceder a los datos de producción solo en casos de emergencia o cuando se requiera.

12. SEGURIDAD EN LA OPERATIVA			
12.1. Protección contra código malicioso	12.1.1.Controles contra el código malicioso.	APLICAR	Actualmente la insitucion tiene herramientas de detección y protección de código malicioso, sin embargo estas no esta documentadas. Para lo cual se debe: - Implementar una política documentada con respecto al uso del correo electrónico e internet. - Capacitar al usuario sobre el uso de los antivirus y cuando haya una infección. Directrices para la prevención de un ataque informático: - Realizar las actualizaciones de los antivirus y sistema operativo periódicamente. - Analizar antes de su uso cualquier medio extraíble. - No abrir correos electrónicos sospechos y borrarlos. - No descargar archivos de dudosa procedencia. - No instalar aplicaciones excepto aquellas que han pasado por un filtro y son recomendadas. - Navegar por sitios de intenert seguro , comprueba que ésta comienza por https://. - No entregar datos reales, email, teléfono, dirección a personas desconocidas y a las que no tienen relación laboralmente. Procedimiento para la eliminación de un virus informático: 1. Apagar el equipo y todos los dispositivos conectados a él. Si el equipo se encuentra conectado a la red se le deberá aislar desconectando el cable de red. 2. Insertar un dispositivo de arranque al

			computador, protegido contra escritura, que contenga el sistema operativo y archivos de detección y eliminación de virus. 3. Rastrear en las unidades adicionales la presencia de virus, especialmente a los discos duros y/o Particiones. 4. Detectados los virus , eliminarlos usando el programa antivirus. 5. De ser posible repetir el paso 3 y 4 para mayor seguridad. 6. Dependiendo de la gravedad del daño ocasionado por el virus, si es necesario, se reinstalará todo el software de la computadora previo backup de los datos del usuario. Este proceso lo debe realizar personal de Soporte Técnico.
12.2. Copias de seguridad .	12.2.1.Copias de seguridad de la información.	APLICAR	Implementar y documentar un procedimiento para la copias de seguridad y recuperación de la información, las cuales tendrán en cuenta las siguientes directrices: - Las copias de respaldo deben abarcar toda la información necesaria para recuperar el servicio en caso de perdida o corrupción de la información.(programas, ficheros de configuración, datos e incluso la imagen del sistema operativo.) - Establecer los periodos de copias mas adecuados para cada tipo de información. - La realización de las copias deben ser realizadas por los usuarios y/o por el servidor. - Almacenar las copias de seguridad en un lugar externo. - La información debe estar cifrada según los procedimientos definidos.

			- La información respaldada en los medios informaticos debe ser verificada al menos una vez al año. - Documentar las pruebas y resultados de la restauración de las copias de seguridad para faciltar un mejor control en su gestión. - Implementar un registro del contenido y ubicación de las copias de seguridad para facilitar un mejor control en su gestión. - Almacenar las copias de seguridad en armarios ignífugos, bajo llave. - Restringuir el acceso a las copias de seguridad, solo el personal previamente autorizado podrá acceder. - El transporte de las copias de seguridad de contar con las medidas de seguridad adecuadas para evitar cualquier robo, alteración o destrucción. Ejemplo: maletines bajo llave y/o mecanismo de cifrado.
12.3. Gestion de la vulnerabilidad Técnica.	12.3.1. Gestion de la vulnerabilidad Técnica.	APLICAR	Implemtar un procedimiento para controlar el acceso a los archivos que contengan información critica sobre los sistemas de información, teniendo en cuenta las siguientes directrices: - Documentar los procedimientos de instalación, mantenimiento y reparación de equipos. - Establecer estánderes de configuración de los puestos de trabajo, servidores y demás equipos . - Realizar chequeos periódicos en las estaciones de trabajo, servidores y demás equipos, en búsqueda de aplicaciones instaladas no autorizadas o incesarias. - Actualizar las aplicaciones solo si se reporta algún mal funcionamiento o a un nuevo requerimiento de los usuarios.

			- Establecer un procedimiento para actualizar peridicamente de los sistemas operativos de las estaciones de trabajo como de los servidores. - Establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados de las aplicaciones o parches y poder recuperar versiones anteriores en caso de generarse problemas.
	12.3.2. Restricción en la instalación de software	Aplicar	- Notificar la prohibición de instalación de cualquier producto de software en los equipos. - Crear cuenta de usuarios de acuerdos a los perfiles requeridos - Restringuir la instalación de utilirarios que pongan en riesgo a los sistemas como software pirata(crack, generadores de claves u otros.) - Solo se permite la instalación de software permitdos por el administrador de sistemas previa autorización documentada. - Restringuir el acceso al código fuente de los sistemas de información .Solo el Administrador de Sistemas y desarrolladores tendrán acceso previo autorización de las autoridades, documentando los accesos y las acciones a realizar.
12.3.Registro de Actividad y Supervición.	12.3.1. Registro y gestión de eventos de seguridad	APLICAR	- Implementar un control para el registro de logs, fallas , excepciones o eventos de seguridad. Dicho registro deberá contener como mínimo: - Nombre de usuario que reportó el incidente. - Fecha y hora del reporte del incdiente - Fecha y hora en la que inicio con las indicaciones - Tipo de sistemas afectados(inlcuido los sistemas operativos y hardware

			relacionado). - Ubicacion del Sistema(dirección ip) - Informar si el evento sigue en curso o tuvo una actuación momentanea - Accions que tomo el usuairo previo al reporte del incidente - Acciones que tomo el area de Soporte Tecnico de la Institucion al tomar conocimiento del incidente - Revisar periódicamente los registros de eventos de seguridad y tomar las medidas requeridas - Analizar periódicamente los siguientes eventos específicos como: - Controles de acceso y permiso de los usuarios, uso de recursos informáticos, operaciones de borrado o modificación de datos en los sistemas o críticos o intentos fallidos de ingreso al sistema. - Actualizar continuamente las herramientas de análisis de logs. - Programar auditorias periódicas y chequeos a aleatorios, para controlar las áreas o funciones criticas con respecto a la seguridad de los datos de la institución, documentando la ejecuacion y resultados de dichas pruebas. - Documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados afectados por la anomalía, reportando a las autoridades pertinentes el incidente y la gravedad, para tomar las acciones necesarias de protección y control de los datos y otras. -

	12.3.2.Protección de los registros de información.	APLICAR	Implentar un control para proteger contra posibles alteraciones y accesos no autorizados la información de los registros. Se deben tener en cuenta las siguientes directrices: - Almacer los registros o log en carpetas de los servidores protegidas con contraseña. - Esta contraseña debe ser desconocida por todos los usuarios del sistema, incluso por el administrador.
	12.3.3.Registro de Actividad del Administrador y operador del Sistema	APLICAR	- Implementar un control para registrar las actividades del administrador y del operador del sistema. - Revisar de forma regular los registros y proteger los accesos. - Realizar controles mas frecuentes sobre los log o registros del Administrador. El estudio de estos reportes debe ser realizado por un superior y no por el administrador.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.			
13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.	APLICADO	La institución mantiene asegurada la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte. Se ha desarrollado mecanismos de seguridad, los niveles de servicio y los requisitos de gestión mínimos de todos los servicios de red.
	13.1.2 Mecanismos de seguridad asociados a servicios en red.	APLICAR	Se sugiere incluir los siguientes controles para mejorar las políticas y procedimientos implementados: - Implementar una política documentada concerniente al uso de redes y servicios de red. Esta debe comprender: - Las redes y servicios de red a los cuales se permite el acceso. - Procedimientos de autorización para

			determinar las personas que tienen permitido el acceso a las redes y los servicios de red. - Controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red. - Los medios utilizados para acceder la red y los servicios de red (condiciones para disponer uso de equipos remotos). - Considerar el uso de técnicas o herramientas para la identificación automática de todos los equipos que se conecten a la red - Etablecer procedimientos formales para monitorear y auditar la correcta gestión de accesos a la red. - Normar la revisión de los acuerdos de servicio con los proveedores de telecomunicaciones, debido a fallas inopinadas o algún tipo de fallas (Naturales o inducidas) comunes en la institución.
	13.1.3 Segregación de redes.	APLICADO	Los grupos de servicios de información, usuarios y sistemas de información se mantienen separados en las redes para así evitar que el tráfico de una subred afecte a las demás.

Fuente: ISO /IEC 27001

CONCLUSIONES

- Se encontró un bajo porcentaje de cumplimiento del 39%, que evidencia un descuido con respecto a la seguridad de la información dentro la institución.
- El modelamiento de los procesos: Caldendarización académica, Inscripción por cursos por semestre, Modificación de nota, Soportede del CIT, Generación de actas evidenció que existe 50 activos e información importante y sensible para la institución.
- Los activos en los procesos académicos analisados presentan un alto valor de criticidad, entre 7 a 9, debido a la confiabilidad, disponibilidad e integridad de éstos para la institución.
- En su mayoría los riesgos asociados a los activos evaluados presentan un valor de riesgo "Alto", los cuales deben mitigados o eliminados, tomando las medidas necesarias por parte de las autoridades de la institución.
- Se ha detectado que existen controles básicos implementados para la seguridad de la información; sin embargo, estos no están documentados ni son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estos controles.

RECOMENDACIONES

- Aquirir los servicios de un especialista que pueda guiar una implementación exitosa de la norma, adoptando las políticas de seguridad de información señaladas en la investigación, debido a que estas se alinean a lo que estipula la norma ISO/IEC 27001, que es un estándar reconocido dentro del ámbito de la seguridad de información.

- Establecer un rol de "Oficial de Seguridad de Información" dentro de la institución para el monitoreo y cumplimiento de las políticas y controles establecidos. Este rol no implica la contratación de personal, sino que puede ser algún personal dentro de la institución que tenga el perfil requerido para dicho rol.

- Capacitar y concientizar a todo el personal de manera periódica con respecto a la seguridad de la información, para lograr que todos los involucrados tengan los mecanismos o procedimientos claros frente a la amenzas o riesgos de seguridad.

- Documentar los procesos académicos para poder gestionarlos de manera óptima y hacer frente a cualquier cambio en la institución. La documentación de procesos también nos permite la mejora de estos.

- Documentar todas las políticas y controles existentes para una mejor gestión de la seguridad de la información en la institución.

- Actualizar periódicamente el Sistema de Gestión de Seguridad de la Información, debido a la posible modificación de las actividades de los procesos, aparición de activos de información y aparición de nuevas amenazas, riesgos.

- Asignar un presupuesto orientado a la implementación del Sistema de Gestión de Seguridad de la Información, así como para las capacitaciones y charlas de concientización, los servicios de consultoría que se darán para asegurar la continuidad del sistema de gestión.

REFERENCIA BIBLIOGRÁFICA

AGUIRRE D.(2014).Diseño de un Sistema de Gestión de Seguridad de Información para SERVICIOS Postales del Perú S.A. Tesis para optar el Título de Ingeniero. Informático.Pontificia Universidad Católica del Perú. Colección de tesis digitales PUCP. Disponible en http://tesis.pucp.edu.pe/repositorio/handle/123456789/933. [Accesado el 23 de octubre del 2018].

ALIAGA L. (2013) Diseño de un Sistema de Gestión de Seguridad de Información para un Instituto Educativo. Tesis para optar el Título de Ingeniero Informático. Pontificia Universidad Católica del Perú. Colección de tesis digitales PUCP. Disponible en: http://tesis.pucp.edu.pe/repositorio/handle/123456789/933. [Accesado 23 de octubre del 2018].

AMPUERO C. (2011). Diseño de un sistema de gestión de seguridad de información para una compañía de seguros. Tesis para optar por el título de Ingeniero. Pontificia Universidad Católica del Perú. Colección de tesis digitales PUCP. Disponible en: http://tesis.pucp.edu.pe/repositorio/handle/123456789/933. [Accesado el 23 de octubre de 2018]

BANCO DE LA NACIÓN (2014). Manuales de Procesos del Banco de la Nación. Disponible en : http://www.bn.com.pe/nosotros/archivos/manual-procesos-bn.pdf. [Accesado el 10 de febrero del 2019].

BARRAGÁN I, GÓNGORA I Y MARTÍNEZ E. (2011), Implementación de Políticas de Seguridad Informática para la M.I. Municipalidad de Guayaquil aplicando la norma ISO/IEC 27002. Tesis de grado. Escuela Superior Politécnica del Litoral. Disponible en: http://www.dspace.espol.edu.ec/handle/123456789/21546. [Accesado el 23 de octubre del 2018].

BSI(s.f). Sistema de gestión ISO/IEC 27001 de Seguridad de la Información.Disponible en: https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/. [Accesado el 15 de diciembre del 2018].

COMISIÓN DE NORMALIZACIÓN Y DE FISCALIZACIÓN DE BARRERAS COMERCIALES NO ARANCELARIAS Y EL INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL - CNB Y INDECOPI(2008).NTP-ISO/IEC27001:2008.Disponible en: http://tamperu.com.pe/brochure/brochure.pdf. [Accesado el 15 de diciembre del 2018]

ESTATUTO DE LA UNIVERSIDAD NACIONAL DE PIURA(2014). Disponible en: http://www.unp.edu.pe/transparenciaunp/down/textounicoestatuto2014incluyemodific.pdf [Accesado el 05 de febrero del 2019].

FRAYSSINET M.(2009). Taller de Gestión de Riesgos. Disponible en: https://www.gobiernodigital.gob.pe/docs/Taller_gestion_de_riesgos.pdf. [Accesado el 20 de marzo del 2019].

INDACOCHEA A. (2013).Una Propuesta para mejorar las prácticas de Gobierno Corporativo en el Perú.Pontificia Universidad Católica Del Perú. Colección de tesis digitales PUCP. Disponible en: https://indacocheanoticias.files.wordpress.com/2013/01/gobierno-corporativo-cladea-03.pdf. [Accesado el 30 noviembre del del 2018].

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL-INDECOPI(2013).Polìtica SIG. Disponible en: https://www.indecopi.gob.pe/politica-sig. [Accesado el 30 de noviembre del 2018].

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL-INDECOPI(2013).NTP ISO/IEC 27001. Disponible en: http://tamperu.com.pe/brochure/brochure.pdf. [Accesado el 10 de enero del 2019].

ISO 27000.es.(2012). El portal de ISO 27001 en Español. Disponible en: http://www.iso27000.es/iso27002.html. [Accesado el 10 de enero del 2019].

ISO 27002.es(2012). Portal de Soluciones Técnicas y Organizativas de referencia a los controles de ISO/IEC27002.Disponible en : http://www.iso27000.es/iso27002.html. [Accesado el 10 de enero del 2019].

ISO/IEC 27001 (2013).Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos. Disponible https://www.iso.org/standard/54534.html. [Accesado el 02 de febrero del 2019].

ISO/IEC 27002(2013).Tecnología de la información-Técnicas de seguridad-Código de práctica para los controles de seguridad de la información. Disponible en: https://www.iso.org/standard/54533.html. [Accesado el 02 de febrero del 2019].

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA (2012). MAGERIT – versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.LibroI–Método. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XHQK4KJKjIU. [Accesado el 03 de marzo del 2019].

NTP ISO/IEC 17799(2007). EDI Tecnología de la información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información- Requisitos. Disponible en: http://www.pecert.gob.pe/_normas/ISO27000/RM-246-2007-PCM.pdf.[Accesado el 25 noviembre del 2018].

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS-COBIT 5(2012).Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa ISACA, USA. Disponible en: https://articulosit.files.wordpress.com/2013/07/cobit5-framework-spanish.pdf .[Accesado el 15 de diciembre del 2018].

RAMÍREZ, A. Y ORTIZ, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. En: Ingeniería, Vol. 16, No. 2, pág. 56-66. Disponible en: https://dialnet.unirioja.es/descarga/articulo/4797252.pd. [Accesado el 20 de febrero del 2019].

REGLAMENTO ACADÉMICO DE LA UNIVERSIDAD NACIONAL DE PIURA (2006). Disponible: http://www.unp.edu.pe/transparenciaunp/down/reglamentoacademicounp25072006unp.pdf. [Accesado el 05 de febrero del 2019].

REGLAMENTO GENERAL DE LA UNIVERSIDAD NACIONAL DE PIURA(2014). Disponible en:http://www.unp.edu.pe/transparenciaunp/down/reglgeneraltextounico2019.pdf. [Accesado el 05 de febrero del 2018]

RESOLUCIÓN MINISTERIAL N° 129-2012-PCM(2012).Presidencia de Consejo de Ministros. Disponible en: http://repositorio.indecopi.gob.pe/bitstream/handle/11724/2625/RM.129-2012-PCM.pdf?sequence=5&isAllowed=y. [Accesado el 20 de Diciembre del 2018].

ROSALES G. (2008). Mejora de la Eficiencia en el Proceso Académico de Matrícula e Inscripción por cursos de la Universidad Nacional de Piura. Disponible en : https://www.academia.edu/4247341/Mejora_de_la_Eficiencia_en_el_Prcoeso_Acad%C3%A9mico_de_Matr%C3%ADcula_e_Inscripci%C3%B3n_por_cursos_en_la_Universidad_Nacional_de_Piura .[Accesado el 25 de enero del 2019].

VILLALÓN A. (2004). Códigos de buenas prácticas de seguridad. UNE-ISO/IEC 17799. Disponible en: http://www.shutdown.es/ISO17799.pd .[Accesado el 07 de noviembre de 2018].

ANEXO Nº1: ANÁLISIS DE DATOS DE CUESTIONARIOS

CUESTIONARIO: DOMINIO DE POLÍTICAS DE SEGURIDAD.

CANTIDAD DE PREGUNTAS CONTESTADAS											
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1	1	2	2	2	2	2	1	2	3	2	2
2	1	2	2	2	2	2	2	2	2	2	2
2	1	2	2	2	2	2	2	2	2	2	1
2	2	2	2	2	2	1	2	2	2	2	2
1	1	2	2	2	2	2	1	2	2	2	2
2	1	2	2	2	2	2	2	2	3	2	3

CUESTIONARIO: DOMINIO ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

CANTIDAD DE PREGUNTAS CONTESTADAS										
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	2	1	1	1	2	2	2	2	3	2
1	3	1	2	1	1	1	1	2	1	2
1	2	1	2	1	2	1	2	2	3	2
2	2	2	2	1	2	2	1	2	2	2
2	2	2	2	1	2	2	2	2	3	2
2	2	2	2	1	2	2	1	2	3	2
2	3	2	2	2	2	2	2	2	3	2
1	3	2	2	1	2	1	2	1	3	2
1	3	1	2	1	1	1	1	1	1	1
2	3	2	2	1	2	1	2	2	3	2
3	3	2	2	1	1	1	1	1	3	1
3	3	1	2	1	2	2	1	2	3	2
2	3	2	2	1	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	3	2
2	1	2	2	2	1	1	2	1	2	1
1	2	2	2	2	2	1	1	2	3	1

1	2	2	2	1	2	2	1	2	3	2
2	2	2	2	1	2	2	2	2	3	1
2	2	2	2	1	2	2	2	2	3	2

DOMINIO: SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

CANTIDAD DE PREGUNTAS CONTESTADAS								
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	2	2	1	2	2	1	1	2
1	2	2	2	2	2	2	2	2
2	2	2	2	2	2	1	1	1
1	3	2	2	2	2	2	2	1
2	1	1	1	2	2	2	2	2
2	2	2	2	2	3	2	2	2

DOMINIO: GESTION DE ACTIVOS

CANTIDAD DE PREGUNTAS CONTESTADAS						
1	**2**	**3**	**4**	**5**	**6**	**7**
1	1	1	1	1	2	1
1	2	1	2	1	2	1
1	1	2	2	1	2	1
1	2	1	1	1	2	1
2	2	2	2	2	2	1
1	1	2	2	2	2	2
2	2	3	2	2	3	2
2	2	2	1	1	3	2
1	2	1	1	2	3	2
1	2	3	1	1	3	2

DOMINIO: SEGURIDAD EN LA TELECOMUNICACIONES

CANTIDAD DE PREGUNTAS CONTESTADAS	
1	**2**
1	1
1	1
1	1
2	1
1	1
1	1
1	1
1	1
1	1
2	1
1	1
1	1
1	1
2	2
1	1
2	2
2	2
1	1
1	1
1	1
2	1
1	1
2	2
2	2
2	2
2	2
1	1
1	1
1	1
1	1
1	1
1	1
2	2
1	1
1	1
1	2
1	1
1	2
1	1
1	1
2	1

2	2
1	1
1	2
1	1
2	1
1	2
1	1
1	2

DOMINIO: CONTROL DE ACCESOS

CANTIDAD DE PREGUNTAS CONTESTADAS					
1	**2**	**3**	**4**	**5**	**6**
2	2	2	2	2	2
1	1	2	1	1	2
1	2	1	2	2	2
1	1	1	2	1	2
1	1	1	1	1	1
1	1	1	2	1	2
1	1	1	1	1	1
1	2	1	2	1	2
1	1	1	1	1	1
2	1	2	2	2	2
1	1	1	1	1	1
1	2	1	1	1	1
2	1	2	2	2	2
1	2	2	1	1	2
1	1	1	1	1	1
1	2	1	2	2	2
1	1	1	1	1	1
2	2	1	1	1	1
1	2	2	2	1	2
2	1	1	2	2	2

DOMINIO SEGURIDAD EN LA OPERATIVA

CANTIDAD DE PREGUNTAS CONTESTADAS		
1	2	3
2	1	2
1	2	1
1	3	1
1	1	1
1	1	1
1	1	1
2	2	2
2	2	2
2	2	2
2	2	2
2	2	2
2	1	2
2	1	2
2	1	1
2	1	2
1	1	1
2	1	2
2	2	2
1	1	1
1	2	1
2	1	2
1	1	1
2	2	2
2	2	1
2	1	1
2	2	2
1	1	1
2	1	1

ANEXO Nº2: CUESTIONARIOS DE LOS DOMINIOS ISO/IEC 27001

DOMNIO: POLITICAS DE SEGURIDAD

INSTITUCION	UNP
CUESTIONARIO DE POLITICA DE LA INFORMACION	D5
DOMINIO	POLÍTICAS DE SEGURIDAD.
OBJETIVO	DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD DE LA INFORMACIÓN
OBJETIVO DE CONTROL	Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.

PREGUNTA	Si	%	No	%	N/A	%	Total
¿Existe una política de seguridad de la información en la Institución?	3	25.00%	8	66.67%	1	8.33%	12
¿Se ha publicado la política de seguridad en la institución?	1	8.33%	11	91.67%	0	0.00%	12
¿Tiene conocimiento de los procedimientos de la Política de seguridad cuando ocurre un evento de seguridad	2	16.67%	10	83.33%	0	0.00%	12
TOTAL	**6**	**16.67%**	**29**	**80.56%**	**1**	**2.77%**	**36**

OBJETIVO	REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
OBJETIVO DE CONTROL	La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.

PREGUNTA	Si	%	No	%	N/A	%	Total
¿Cuenta con definiciones de sanciones orgánicas para la violación de políticas y procedimientos de seguridad.	1	8.33%	11	91.67%	0	0.00%	12
¿Existe una planificación y revisión con regularidad o si existen cambios significativos de la política de la seguridad de la información?	3	25.00%	9	75.00%	0	0.00%	12
¿Está alineada a los objetivos de la institución la política de seguridad?	1	8.33%	9	75.00%	2	16.67%	12
TOTAL	**5**	**13.88%**	**29**	**80.56%**	**2**	**5.56%**	**36**

DOMINIO: ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

INSTITUCIÓN		UNP					
CUESTIONARIO DE CONTROL DE ORGANIZACION INTERNA		D6					
DOMINO	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN						
OBJETIVO	ORGANIZACIÓN INTERNA						
OBJETIVO DE CONTROL	El objetivo es el de establecer un esquema directivo de gestión para iniciar y controlar la implementación y operativa de la seguridad de la información en la organización.						
PREGUNTA	**Si**	**%**	**No**	**%**	**N/A**	**%**	**Total**
¿Hay una persona en la organización que sea responsable de la seguridad de la información y tenga como debe principal mantener el plan de seguridad y garantizar su cumplimiento?	4	36.36%	6	54.55%	1	9.09%	11
¿El jefe y el personal de su organización tienen la experiencia y calificación necesaria en seguridad de la información?	7	63.64%	3	27.27%	1	9.09%	11
¿Tiene el personal de los sistemas de información una responsabilidad específica asignada para la ejecución de la continuidad y los planes de recuperación de desastres?	4	36.36%	6	54.55%	1	9.09%	11
¿Existe un programa de capacitación permanente para desarrollar habilidades y competencias para la seguridad de la información al personal encargado de los sistemas de información?	2	18.18%	9	81.82%	0	0.00%	11
¿Existe un comité de Seguridad de la información formado por las áreas de la institución?	1	9.09%	9	81.82%	1	9.09%	11
¿El personal que la labora tiene asignada roles o responsabilidades sobre la seguridad de la información?	2	18.18%	8	72.73%	1	9.09%	11
¿Existe un oficial de seguridad de la información en la institución?	0	0.00%	9	81.82%	2	18.18%	11
¿Hay una segregación de tareas y áreas de responsabilidad ante posibles conflictos?	4	36.36%	5	45.46%	2	18.18%	11

¿Se mantiene los contactos apropiados con las autoridades pertinentes que impliquen la comunicación, cooperación y colaboración con los directores, jefes de área, administradores, usuarios, etc.?	9	81.82%	1	9.09%	1	9.09%	11
¿Se desarrolla contacto con especialistas externos en seguridad para mantener actualizado en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como proporcionar enlaces adecuados para el tratamiento de las incidencias de seguridad?	2	18.18%	7	63.64%	2	18.18%	11
¿Se contempla la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización?	6	54.55%	2	18.18%	3	27.27%	11
¿El personal de los sistemas de información participa activamente con otras oficinas (OCRA, Recursos Humanos, Planificación, etc.) para verificar y hacer cumplir las políticas de seguridad de la información?	3	27.27%	5	45.45%	3	27.27%	11
¿Ha implementad una educación y concientización en seguridad de la información?	1	9.09%	9	81.82%	1	9.09%	11
¿Cuenta con la declaración firmada por todo el personal responsable del uso de los sistemas de información con respecto a la confidencialidad de la información?	0	0.00%	10	90.91%	1	9.09%	11
¿Existe un diseño inadecuado de la estrategia organización?	5	45.45%	6	54.55%	0	0.00%	11
¿Los problemas de seguridad de la información está considerada en todas las decisiones importantes dentro de la organización?	4	36.36%	6	54.55%	1	9.09%	11
TOTAL	**54**	**30.68%**	**101**	**57.39%**	**21**	**11.93%**	**176**

OBJETIVO	0DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO
OBJETIVO DE CONTROL	El objetivo es el de garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.

Pregunta	Si	%	No	%	N/A	%	Total
¿Existe una política formal y medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones?	3	27.27%	7	63.64%	1	9.09%	11
¿Existe políticas claramente definidas para la protección, no sólo de los propios equipos informáticos, sino, en mayor medida, de la información almacenada en ellos?	2	18.18%	8	72.73%	1	9.09%	11
¿Existe política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo.?	1	9.09%	9	81.82%	1	9.09%	11
TOTAL	**6**	**18.18%**	**24**	**72.73%**	**3**	**9.09%**	**33**

DOMINIO: CUESTIONARIO DE CONTROL DE SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

INSTITUCIÓN	UNP
CUESTIONARIO DE CONTROL DE SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	D7
DOMINO	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
OBJETIVO	ANTES DE CONTRATACIÓN
OBJETIVO DE CONTROL	El objetivo es el de asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen, proteger los intereses de la Institución. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

Pregunta	Si	%	No	%	N/A	%	Total
¿Antes de la contratación laboral se le describió adecuadamente el trabajo que iba a realizar y los términos y condiciones del empleo con relación a la seguridad?	4	44.44%	5	55.56%	0	0.00%	9
¿Ha firmado un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad?	1	11.11%	8	88.89%	0	0.00%	9

TOTAL	**5**	**27.78%**	**13**	**72.22%**	**0**	**0.00%**	**18**
OBJETIVO	DURANTE LA CONTRATACIÓN						
OBJETIVO DE CONTROL	El objetivo es el de asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.						
PREGUNTA	**Si**	**%**	**No**	**%**	**N/A**	**%**	**Total**
¿Se ha proporcionado un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad?	3	33.33%	6	66.67%	0	0.00%	9
¿En su contrato laboral especifica un proceso disciplinario normal para gestionar las brechas de seguridad?	2	22.22%	6	66.67%	1	11.11 %	9
TOTAL	**5**	**27.78%**	**12**	**66.67%**	**1**	**5.55%**	18
OBJETIVO	Cese o cambio de puesto de trabajo						
OBJETIVO DE CONTROL	El objetivo es el de proteger los intereses de la organización durante el proceso de cambio o finalización de empleo por parte de empleados y contratistas.						
PREGUNTA	**Si**	**%**	**No**	**%**	**N/A**	**%**	**Total**
¿Tiene una política de devolución de activos cuando cesa su contrato laboral?	3	33.33%	6	66.67%	0	0.00%	9
¿Tiene acceso parcial a los activos aun cuando su contrato ya finalizó (e-mails, sistemas, datos, etc.?	0	0.00%	8	88.89%	1	11.11 %	9
TOTAL	**3**	**16.67%**	**14**	**77.78%**	**1**	**5.55%**	**18**

DOMINIO: GESTIÓN DE ACTIVOS

INSTITUCIÓN	UNP						
CUESTIONARIO DE GESTION DE ACTIVOS	D8						
DOMINO	GESTION DE ACTIVOS						
OBJETIVO	RESPONSABILIDAD SOBRE LOS ACTIVOS						
OBJETIVO DE CONTROL	El objetivo es identificar los activos en la organización y definir las responsabilidades para una protección adecuada.						
PREGUNTA	**Si**	**%**	**No**	**%**	**N/A**	**%**	**Total**
¿Se tiene un inventario de activos?	6	85.71%	1	14.29%	0	0.00%	7
¿Todos los activos están claramente identificados?	4	57.14%	3	42.86%	0	0.00%	7
¿Se revisa frecuentemente el inventario?	4	57.14%	3	42.86%	0	0.00%	7
¿Existe una persona encargada o propietario asignada por dirección para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos?	5	71.43%	2	28.57%	0	0.00%	7
TOTAL	**19**	**67.86%**	**9**	**32.14%**	**0**	**0.00%**	**28**
OBJETIVO	CLASIFICACIÓN DE LA INFORMACIÓN						
OBJETIVO DE CONTROL	El objetivo es el de asegurar que se aplica un nivel de protección adecuado a la información.						
PREGUNTA	**Si**	**%**	**No**	**%**	**N/A**	**%**	**Total**
¿Existe información documentada sobre el uso adecuado de los activos y tratamiento de información?	2	28.57%	5	71.43%	0	0.00%	7
¿Se posee de bitácoras de fallas detectadas en los equipos?	0	0.00%	5	71.43%	2	28.57%	7
¿Usa códigos de barras para facilitar las tareas de realización de inventario y para vincular equipos de TI que entran y salen de las instalaciones con empleados?	1	14.29%	6	85.71%	0	0.00%	7
TOTAL	**3**	**14.29%**	**16**	**76.19%**	**2**	**9.52%**	**21**

OBJETIVO	MANEJO DE LOS SOPORTES DE ALMACENAMIENTO
OBJETIVO DE CONTROL	El objetivo es evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento.

PREGUNTA	**Si**	**%**	**No**	**%**	**N/A**	**%**	**Total**
¿Existe procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas?	2	28.57%	4	57.15%	1	14.28%	7
¿Los soportes de almacenamiento y la información en tránsito no solo físico sino electrónico (a través de las redes) están protegidos en cuanto robo, destrucción, modificación, etc.?	3	42.86%	3	42.86%	1	14.28%	7
¿Los activos sensibles o valiosos están cifrados antes de ser transportados por la red?	3	42.86%	2	28.57%	2	28.57%	7
TOTAL	**8**	**38.09%**	**9**	**42.86%**	**4**	**19.05%**	**21**

DOMINIO: CONTROL DE ACCESOS

INSTITUCIÓN	UNP
CUESTIONARIO DE CONTROL DE ACCESOS	D9
DOMINO	CONTROL DE ACCESOS
OBJETIVO	REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS
OBJETIVO DE CONTROL	El objetivo es controlar los accesos a la información y las instalaciones utilizadas para su procesamiento

Pregunta	**Si**	**%**	**No**	**%**	**N/A**	**%**	**TOTAL**
¿Existe una política de control de acceso documentada?	0	0.00%	6	100.00%	0	0.00%	6
¿Existe un procedimiento de identificación y autenticación?	4	66.67%	2	33.33%	0	0.00%	6
¿Existen controles para el acceso a los recursos?	2	33.33%	4	66.67%	0	0.00%	6
TOTAL	**6**	**33.33%**	**12**	**66.67%**	**0**	**0.00%**	**18**

OBJETIVO	GESTIÓN DE ACCESO DE USUARIO
OBJETIVO DE CONTROL	El objetivo es el de garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.

PREGUNTA	Si	%	No	%	N/A	%	Total
¿Se cumple con los requisitos de control de acceso, la autentificación y autorización de usuarios?	4	66.67%	2	33.33%	0	0.00%	6
¿Existe niveles de usuarios para el acceso a los sistemas y servicios de información?	6	100.00%	0	0.00%	0	0.00%	6
¿Cuenta con procedimientos de baja y alta de usuarios?	4	66.67%	2	33.33%	0	0.00%	6
¿Existe un administrador de sistemas que controle las cuentas de los usuarios?	6	100.00%	0	0.00%	0	0.00%	6
Una vez pasados los filtros ¿Se han separado los recursos a los que tiene acceso cada usuario?	3	50.00%	3	50.00%	0	0.00%	6
¿Los usuarios de bajo nivel tienen restringido el acceso a las partes más delicadas de las aplicaciones?	6	100.00%	0	0.00%	0	0.00%	6
TOTAL	**29**	**80.56%**	**7**	**19.44%**	**0**	**0.00%**	**36**

OBJETIVO	RESPONSABILIDADES DEL USUARIO
OBJETIVO DE CONTROL	El objetivo es hacer que los usuarios sean responsables de la protección de la información para su identificación

PREGUNTA	Si	%	No	%	N/A	%	TOTAL
¿Se ha definido y documentado claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo?	1	16.67%	5	83.33%	0	0.00%	6
¿Es consciente de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición?	6	100.00%	0	0.00%	0	0.00%	6
TOTAL	**7**	**58.33%**	**5**	**41.67%**	**0**	**0.00%**	**12**

OBJETIVO	CONTROL DE ACCESO A SISTEMAS Y APLICACIONES
OBJETIVO DE CONTROL	El objetivo es impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.

Pregunta	**Si**	**%**	**No**	**%**	**N/A**	**%**	**Total**
¿Se ha implementado claves o password para utilizar operación de consola y equipo central (servidor) al personal autorizado?	5	83.33%	1	16.67%	0	0.00%	6
¿Las contraseñas se asignan de forma automática por el servidor?	1	16.67%	5	83.33%	0	0.00%	6
¿Existe un procedimiento de cambio de contraseñas?	3	50.00%	3	50.00%	0	0.00%	6
¿Existe un procedimiento seguro de login para el acceso a los sistemas y aplicaciones?	6	100.00%	0	0.00%	0	0.00%	6
¿Se controla y restringe el uso de utilidades de software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas?	2	33.33%	4	66.67%	0	0.00%	6
¿El personal autorizado tiene el acceso al código fuente de las aplicaciones de software?	6	100.00%	0	0.00%	0	0.00%	6
¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?	4	66.67%	2	33.33%	0	0.00%	6
¿Los practicantes pre y – Profesionales cuentan con funciones y responsabilidades específicas?	2	33.33%	4	66.67%	0	0.00%	6
¿Se permite el acceso a los archivos y programas a los practicantes pre-profesionales?	2	33.33%	4	66.67%	0	0.00%	6
TOTAL	**31**	**57.41%**	**23**	**42.59%**	**0**	**0.00%**	**54**

DOMINIO: SEGURIDAD EN LA OPERATIVA

INSTITUCIÓN			UNP				
CUESTIONARIO DE BASE DE DATOS			D12				
DOMINO	SEGURIDDAD EN LA OPERATIVA						
OBJETIVO	COPIAS DE SEGURIDAD						
OBJETIVO DE CONTROL	El objetivo es alcanzar un grado de protección deseado contra la pérdida de datos.						
PREGUNTA	**Si**	**%**	**No**	**%**	**N/A**	**%**	**Total**
¿Se tiene un responsable de SGBD?	1	33.33%	2	66.67%	0	0.00%	3
¿Existe algún usuario que no sea el DBA pero que tenga asignado el rol DBA del servidor?	2	66.67%	1	33.33%	0	0.00%	3
¿Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?	2	66.67%	0	0.00%	1	33.33%	3
¿Se realiza copias de seguridad?	3	100.00 %	0	0.00%	0	0.00%	3
¿Existe un procedimiento de copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?	3	100.00 %	0	0.00%	0	0.00%	3
¿Las copias de seguridad se efectúan diariamente?	3	100.00 %	0	0.00%	0	0.00%	3
¿Existe controles sobre el acceso físico a las copias de seguridad?	0	0.00%	3	100.00%	0	0.00%	3
¿Se almacenan las copias de seguridad en un lugar de acceso restringido?	0	0.00%	3	100.00%	0	0.00%	3
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?	0	0.00%	3	100.00%	0	0.00%	3
¿Las copias de seguridad son encriptados?	0	0.00%	3	100.00%	0	0.00%	3
TOTAL	**14**	**46.67%**	**15**	**50.00%**	**1**	**3.33%**	**30**

OBJETIVO	PROTECCIÓN CONTRA CÓDIGO MALICIOSO
OBJETIVO DE CONTROL	El objetivo es garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware

PREGUNTA	**Si**	**%**	**No**	**%**	**N/A**	**%**	**Total**
¿ Tiene un software de antivirus en la organización?	3	100.00%	0	0%	0	0%	3
¿Se encuentra actualizado el software antivirus?	1	33.33%	0	0.00%	2	66.67%	3
¿ Se ha realizado un plan de capacitación y actualización frente a las nuevas amenazas o peligros de los códigos maliciosos como el robo y destrucción de la información o daños e inutilización de los sistemas de la organización?	0	0.00%	3	100.00%	0	0.00%	3
¿Existe políticas documentas sobre el uso correcto de email o correo electrónico dentro de la institución u otras medios de mensajería instánea.	0	0.00%	3	100.00%	0	0.00%	3
¿Exite un plan de recuperación de los sistemas o información frente una afección o amenaza de un malware?	0	0.00%	3	100.00%	0	0.00%	3
TOTAL	**4**	**26.67%**	**9**	**60.00%**	**2**	**13.33%**	**15**

OBJETIVO	GESTIÓN DE LA VULNERABILIDAD TÉCNICA
OBJETIVO DE CONTROL	El objetivo es evitar la explotación de vulnerabilidades técnicas

PREGUNTA	**Si**	**%**	**No**	**%**	**N/A**	**%**	**Total**
¿Existe controles de restricción para la instalación de software?	0	0.00%	3	100.00%	0	0.00%	3
¿Existen nivel de usuarios en los sistemas académicos?	3	100.00 %	0	0.00%	0	0.00%	3
¿Se tiene politicas de contraseñas seguras?	0	0.00%	3	100.00%	0	0.00%	3
¿Existen registros de seguridad de las	0	0.00%	3	100.00%	0	0.00%	3

modificaciones o cambios realizados en los sistemas académicos?							
¿Existen registros de seguridad de los accesos a los sistemas y/o sistemas académicos?	0	0.00%	3	100.00%	0	0.00%	3
¿Se ha capacitado a los usuarios en el uso de los sistemas?	3	100.00 %	0	0.00%	0	0.00%	3
¿Se realizan parches de seguridad o actualizaciones a los sistemas operativos o aplicaciones.?	0	0.00%	3	100.00%	0	0.00%	3
TOTAL	**6**	**28.57%**	**15**	**71.43%**	**0**	**0.00%**	**21**

OBJETIVO	REGISTRO DE ACTIVIDAD Y SUPERVISIÓN
OBJETIVO DE CONTROL	El objetivo es registrar los eventos relacionados con la seguridad de la información y generar evidencias

PREGUNTA	**Si**	**%**	**No**	**%**	**N/A**	**%**	**Total**
¿Existe un programa de mantenimiento preventivo para el dispositivo del SGBD?	0	0.00%	3	100.00%	0	0.00%	3
¿Se tiene relación del personal autorizado para manipular la BD?	1	33.33%	2	66.67%	0	0.00%	3
¿Son gestionados los perfiles de estos usuarios por el administrador?	1	33.33%	2	66.67%	0	0.00%	3
¿Son gestionados los accesos a las instancias de la Base de Datos?	2	66.67%	1	33.33%	0	0.00%	3
¿Las instancias que contienen el repositorio, tienen acceso restringido?	1	33.33%	2	66.67%	0	0.00%	3
¿Se renuevan las claves de los usuarios de la Base de Datos?	3	100.00 %	0	0.00%	0	0.00%	3
¿Se obliga el cambio de la contraseña de forma automática?	1	33.33%	2	66.67%	0	0.00%	3
¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras,	0	0.00%	3	100.00%	0	0.00%	3

tablas físicas y lógicas del repositorio?							
¿Posee la base de datos un diseño físico y lógico?	3	100.00 %	0	0.00%	0	0.00%	3
¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?	2	66.67%	1	33.33%	0	0.00%	3
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?	1	33.33%	2	66.67%	0	0.00%	3
¿Cuándo se necesita restablecer la base de datos, se le comunica al Administrador?	3	100.00 %	0	0.00%	0	0.00%	3
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?	0	0.00%	3	100.00%	0	0.00%	3
¿Se documentan los cambios efectuados?	1	33.33%	2	66.67%	0	0.00%	3
¿Hay algún procedimiento para dar de alta/ baja a un usuario?	2	66.67%	1	33.33%	0	0.00%	3
¿Es eliminada la cuenta del usuario en dicho procedimiento?	0	0.00%	3	100.00%	0	0.00%	3
¿El motor de Base de Datos soporta herramientas de auditoría?	3	100.00 %	0	0.00%	0	0.00%	3
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	2	66.67%	1	33.33%	0	0.00%	3
TOTAL	**26**	**48.15%**	**28**	**51.85%**	**0**	**0.00%**	**54**

DOMINIO: SEGURIDAD EN LAS TELECOMUNICACIONES

INSTITUCIÓN	UNP
CUESTIONARIO DE CONTROL: SEGURIDAD EN LAS TELECOMUNICACIONES.	D13

DOMINO	SEGURIDAD EN LAS TELECOMUNICACIONES
OBJETIVO	Gestión de la seguridad en las redes
OBJETIVO DE CONTROL	El objetivo es evitar el acceso físico y lógico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.

PREGUNTA	Si	%	No	%	N/A	%	Total
¿Todos los nodos se encuentran bajo un mismo estándar de modo que no se reduzca la velocidad de transmisión?	2	100.00%	0	0.00%	0	0.00%	2
¿Se gestiona la infraestructura de la red inalámbrica en base a los recursos de radiofrecuencia de los clientes?	2	100.00%	0	0.00%	0	0.00%	2
¿Los enlaces de la red se testean frecuentemente?	2	100.00%	0	0.00%	0	0.00%	2
¿La longitud de los tramos de cableado horizontal no excede de los 90 metros?	1	50.00%	1	50.00%	0	0.00%	2
¿El armado del patch panel cumple con los requerimientos básicos del estándar 568-A y 568-B?	2	100.00%	0	0.00%	0	0.00%	2
Cuenta con un mapa arquitectónico para la verificación del sembrado de nodos?	2	100.00%	0	0.00%	0	0.00%	2
¿El cable cuenta con los recorridos horizontales correctos para el backbone y sus subsistemas?	2	100.00%	0	0.00%	0	0.00%	2
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?	2	100.00%	0	0.00%	0	0.00%	2
¿Cuenta con dispositivo firewall de hardware y software para protección y aseguramiento de la red?	2	100.00%	0	0.00%	0	0.00%	2
¿Actualmente se encuentra vulnerable ante ataques a su red loca, tales como virus, intrusos, malwares, etc.?	1	50.00%	1	50.00%	0	0.00%	2
¿Ha establecido políticas sobre redes?	2	100.00%	0	0.00%	0	0.00%	2

¿Ha definido políticas sobre los puntos de acceso?	2	100.00%	0	0.00%	0	0.00%	2
¿Tiene mecanismo de autenticación de usuarios?	2	100.00%	0	0.00%	0	0.00%	2
¿Tiene herramientas de detección de Spyware/Spam?	0	0.00%	2	100.00%	0	0.00%	2
¿Tiene Herramientas de detección de código malicioso?	2	100.00%	0	0.00%	0	0.00%	2
¿Existe sistema de detección de intrusos (IDS)?	0	0.00%	2	100.00%	0	0.00%	2
¿Existe sistema de prevención de intrusos (IPS)?	0	0.00%	2	100.00%	0	0.00%	2
¿Tiene filtros de contenido?	2	100.00%	0	0.00%	0	0.00%	2
¿Los problemas que exponen la seguridad de sus red local son principalmente debido a los usuarios (ataques internos)?	2	100.00%	0	0.00%	0	0.00%	2
¿Existen sistemas operativos servidores que impiden el acceso a los datos a los usuarios no autorizados?	2	100.00%	0	0.00%	0	0.00%	2
¿Protege su antivirus los correos electrónicos y la descarga de archivos vía web?	1	50.00%	1	50.00%	0	0.00%	2
¿Disponen de correo electrónico corporativo todos los usuarios?	2	100.00%	0	0.00%	0	0.00%	2
¿De aquellos que disponen se le ha informado de la política de la institución en cuanto a su uso?	0	0.00%	2	100.00%	0	0.00%	2
¿Existe una política definida para el acceso a internet?	0	0.00%	2	100.00%	0	0.00%	2
¿Se ha explicado claramente al personal de su organización?	0	0.00%	2	100.00%	0	0.00%	2
¿Existe una política definida para el acceso a internet corporativo?	0	0.00%	2	100.00%	0	0.00%	2
¿Está limitado el acceso por el puesto?	2	100.00%	0	0.00%	0	0.00%	2
¿Está limitado el acceso por usuario?	2	100.00%	0	0.00%	0	0.00%	2
¿Existen controles sobre las páginas accedidas por cada usuario o puesto para tomar medidas contra el usuario que no cumpla sus funciones?	2	100.00%	0	0.00%	0	0.00%	2
¿Existen controles sobre intrusiones externas en nuestro sistema de información?	2	100.00%	0	0.00%	0	0.00%	2
¿Existe un inventario de equipos y software asociado a las redes de datos?	2	100.00%	0	0.00%	0	0.00%	2
¿Dispone de Web Site Empresarial?	2	100.00%	0	0.00%	0	0.00%	2

¿Se ha contratado el hosting a una empresa externa?	0	0.00%	2	100.00%	0	0.00%	2
¿Se realiza el mantenimiento por el personal de la propia empresa?	2	100.00%	0	0.00%	0	0.00%	2
¿Está alojado en la red empresarial el servidor Web?	2	100.00%	0	0.00%	0	0.00%	2
¿Existen controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red?	1	50.00%	1	50.00%	0	0.00%	2
¿Existen procedimientos adecuados para conectarse y desconectarse de los equipos remotos?	2	100.00%	0	0.00%	0	0.00%	2
¿Cuentan con conmutadores en red, para la expansión de redes locales?	1	50.00%	1	50.00%	0	0.00%	2
¿Se tiene conexión a tierra física (pozo a tierra) para protección de equipos ante posibles descargas eléctricas que puedan afectar?	2	100.00%	0	0.00%	0	0.00%	2
¿Se tiene implementado un sistema de control de acceso a los centros de cableado y dispositivos?	2	100.00%	0	0.00%	0	0.00%	2
¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?	1	50.00%	1	50.00%	0	0.00%	2
¿Esta implementado un modelo de QoS en la red?	0	0.00%	2	100.00%	0	0.00%	2
¿La red cuenta con los equipos y aplicaciones (protección) necesarias para tener una mayor resguardo de intrusos activos (hackers)?	2	100.00%	0	0.00%	0	0.00%	2
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?	1	50.00%	1	50.00%	0	0.00%	2
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?	2	100.00%	0	0.00%	0	0.00%	2
¿Los datos que viajan por internet se encuentran cifrados?	1	50.00%	1	50.00%	0	0.00%	2
En cuanto a las pruebas y seguridad de la red, ¿el departamento de TI, genera sus propios ataques para probar la solidez de la red y encontrar posibles fallas?	1	50.00%	1	50.00%	0	0.00%	2

Cuentan con administración interna de la red es decir, ¿Cuentan con VLAN's creadas en el servidor para tener una mayor administración en cada una de las oficinas que se dedican a diferentes actividades?	2	100.00%	0	0.00%	0	0.00%	2
Para evitar vulnerabilidades en las WLAN ¿Usan protocolos de autenticación, como está establecido en el estándar IEEE 802.11?	1	50.00%	1	50.00%	0	0.00%	2
TOTAL	**70**	**71.43%**	**28**	**28.57%**	**0**	**0.00%**	**98**

ANEXO Nº3: LISTA DE EJEMPLOS DE VULNERABILIDADES Y AMENAZAS

Tipo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información
	Falta de esquemas de reemplazo periódico.	Destrucción del equipo o los medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Falta de control de cambio con configuración eficiente	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Falta de pruebas de auditoría	Abuso de los derechos
	Distribución errada de los derechos de acceso	Abuso de los derechos
	Software de distribución amplia	Corrupción de datos
	Utilización de los programas de aplicación a los datos errados en términos de tiempo	Corrupción de datos
	Interface de usuario complicada	Error en el uso
	Falta de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Falta de control eficaz del cambio	Mal funcionamiento del software

	Descarga y uso no controlados de software	Manipulación con software
	Falta de copias de respaldo	Manipulación con software
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
	Falta de prueba del envío o la recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha de la comunicación
	Tráfico sensible sin protección	Escucha de la comunicación
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Arquitectura insegura de la red	Espionaje remoto
	Falta de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Transferencia de contraseñas autorizadas	Espionaje remoto
	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo

ANEXO Nº4: CONTROLES ISO/IEC 27002

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.
- 5.1.1 Conjunto de políticas para la seguridad de la información.
- 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.
- 6.1.1 Asignación de responsabilidades para la segur. de la información.
- 6.1.2 Segregación de tareas.
- 6.1.3 Contacto con las autoridades.
- 6.1.4 Contacto con grupos de interés especial.
- 6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.
- 6.2.1 Política de uso de dispositivos para movilidad.
- 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.
- 7.1.1 Investigación de antecedentes.
- 7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.
- 7.2.1 Responsabilidades de gestión.
- 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
- 7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.
- 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.
- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 8.1.3 Uso aceptable de los activos.
- 8.1.4 Devolución de activos.

8.2 Clasificación de la información.
- 8.2.1 Directrices de clasificación.
- 8.2.2 Etiquetado y manipulado de la información.
- 8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.
- 8.3.1 Gestión de soportes extraíbles.
- 8.3.2 Eliminación de soportes.
- 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.
- 9.1.1 Política de control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.
- 9.2.1 Gestión de altas/bajas en el registro de usuarios.
- 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
- 9.2.4 Gestión de información confidencial de autenticación de usuarios.
- 9.2.5 Revisión de los derechos de acceso de los usuarios.
- 9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.
- 9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.
- 9.4.1 Restricción del acceso a la información.
- 9.4.2 Procedimientos seguros de inicio de sesión.
- 9.4.3 Gestión de contraseñas de usuario.
- 9.4.4 Uso de herramientas de administración de sistemas.
- 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

10.1 Controles criptográficos.
- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.
- 11.1.1 Perímetro de seguridad física.
- 11.1.2 Controles físicos de entrada.
- 11.1.3 Seguridad de oficinas, despachos y recursos.
- 11.1.4 Protección contra las amenazas externas y ambientales.
- 11.1.5 El trabajo en áreas seguras.
- 11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.
- 11.2.1 Emplazamiento y protección de equipos.
- 11.2.2 Instalaciones de suministro.
- 11.2.3 Seguridad del cableado.
- 11.2.4 Mantenimiento de los equipos.
- 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 11.2.8 Equipo informático de usuario desatendido.
- 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.
- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.
- 12.1.3 Gestión de capacidades.
- 12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.
- 12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.
- 12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.
- 12.4.1 Registro y gestión de eventos de actividad.
- 12.4.2 Protección de los registros de información.
- 12.4.3 Registros de actividad del administrador y operador del sistema.
- 12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.
- 12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.
- 12.6.1 Gestión de las vulnerabilidades técnicas.
- 12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.
- 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.
- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.
- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES | CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.
- 14.2.1 Política de desarrollo seguro de software.
- 14.2.2 Procedimientos de control de cambios en los sistemas.
- 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 14.2.4 Restricciones a los cambios en los paquetes de software.
- 14.2.5 Uso de principios de ingeniería en protección de sistemas.
- 14.2.6 Seguridad en entornos de desarrollo.
- 14.2.7 Externalización del desarrollo de software.
- 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- 14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.
- 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.
- 15.1.1 Política de seguridad de la información para suministradores.
- 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
- 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.
- 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
- 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras.
- 16.1.1 Responsabilidades y procedimientos.
- 16.1.2 Notificación de los eventos de seguridad de la información.
- 16.1.3 Notificación de puntos débiles de la seguridad.
- 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
- 16.1.5 Respuesta a los incidentes de seguridad.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.
- 17.1.1 Planificación de la continuidad de la seguridad de la información.
- 17.1.2 Implantación de la continuidad de la seguridad de la información.
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.
- 18.1.1 Identificación de la legislación aplicable.
- 18.1.2 Derechos de propiedad intelectual (DPI).
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.
- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento de las políticas y normas de seguridad.
- 18.2.3 Comprobación del cumplimiento.

ISO27002

ANEXO Nº5.: POLITICAS Y/O DIRECTIVAS DE CIT- UNP

DIRECTIVA N°001-2015-CIT-UNP

RECOMENDACIONES TÉCNICAS PARA LA ORGANIZACIÓN, IMPLEMENTACION Y GESTIÓN DE SERVICIOS INFORMÁTICOS EN LA UNIVERSIDAD NACIONAL DE PIURA

CIT-001 Directiva de Organización, Implementación y Gestión de Servicios Informáticos			
Serie:	Directiva	**Preparado por:**	Unidad de Desarrollo
Versión:	1.0	**Revisado por:**	Ing. Jonathan Nima Ramos
Fecha:	Agosto 2015	**Aprobado por:**	Ing. Wilfredo Cruz Yarlequé

CONSIDERANDO

Que, siendo el Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura responsable del funcionamiento de los sistemas informáticos de la institución y por ende responsable de conducir y supervisar el uso de tecnologías, evaluar métodos, procedimientos y técnicas usadas en la implementación de soluciones que busquen en todo momento el desarrollo de la actividad informática dentro de nuestra Universidad, con el fin de promover el desarrollo, eficiencia y el beneficio de la institución bajo la aplicación de una normativa clara y concisa.

SE DETERMINA:

Elaborar la directiva N°001-2015-CIT-UNP "RECOMENDACIONES TÉCNICAS PARA LA ORGANIZACIÓN, IMPLEMENTACIÓN Y GESTIÓN DE LOS SERVICIOS INFORMÁTICOS EN LA UNIVERSIDAD NACIONAL DE PIURA", la cual deberá ser evaluada y aprobada por las autoridades correspondientes a la presente gestión, para su inmediata aplicación.

I. FINALIDAD

Brindar las recomendaciones técnicas y funcionales que deberán tenerse en cuenta para una adecuada organización, administración, evaluación de todo servicios informático que se desee implementar en cualquier dependencia de la Universidad Nacional de Piura.

II. OBJETIVO

2.1 Orientar la adecuada organización de todo Servicio Informático con los que la institución desea disponer.

2.2 Dar pautas para una mejor gestión de los Servicios Informáticos con los que la institución ya dispone.

2.3 Establecer criterios de evaluación de los Servicios Informáticos con los que la institución desea implementar.

III. ALCANCE

Comprende a todas las dependencias de la Universidad que deseen hacer uso de sistemas informáticos, que ya posean uno o varios sistemas informáticos y a todo el personal que hace uso de equipos informáticos en la Universidad Nacional de Piura.

IV. DISPOSICIONES GENERALES

DE LA GESTIÓN TÉCNICA DE UN SERVICIO INFORMÁTICO

5.1 Los que controlan, usan y/o requieren un Servicio Informático:

a. El Centro de Informática y Telecomunicaciones, en adelante **CIT**, dependencia responsable del procesamiento automático de datos y del control de todo el parque informático de la Universidad, tanto a nivel de hardware, software y comunicaciones, se caracteriza por disponer de equipos de procesamiento de datos de gran capacidad operativa. A esta dependencia por su nivel de responsabilidad y función le corresponde la planeación, organización, desarrollo y mantenimiento de todos los servicios informáticos de la Universidad, por lo que su gestión está basada sobre áreas especializadas, tales como:

- **La Dirección General**, encargada de dirigir, evaluar y controlar la funcionalidad y operatividad del CIT, en el marco de la eficacia y eficiencia del servicio. Así como de la supervisión del desarrollo de proyectos informáticos realizados por el Área de Desarrollo de Sistemas y por terceros.
- **Área de Desarrollo de Sistemas**, responsable de las actividades de planeamiento, análisis, diseño, programación y mantenimiento de Sistemas Informáticos para lo cual requiere de personal especializado en esta tarea.
- **Área de Redes y Comunicaciones**, implementa los controles adecuados que permiten mantener la integridad, seguridad y conectividad (interna como externa) de los equipos informáticos; salvaguardando la integridad, respaldo y restauración eficiente de la información de los mismos, además de especificar los procedimientos necesarios que permitan su conservación.
- **Área de Soporte Técnico**, responsable de prestar apoyo técnico, operativo, de producción, de seguridad de sistemas y datos, así como de la capacitación a los usuarios que hagan uso de un servicio informático.
- **Área de Servicio a los Usuarios**, esta dependencia existirá cuando el grado de desarrollo y crecimiento de la institución haga necesario separar estas actividades del Área de Soporte Técnico, y por tanto se responsabilizará de coordinar políticas y normas, y brindará apoyo y asesoramiento a todos usuarios que hagan uso de los servicios informáticos.

b. **Unidades Operativas**, son funcionalmente, dependencias orientadas a efectuar actividades de procesamiento automático de datos, y a la ejecución de aplicaciones específicas y/o especializadas, de autoedición, están asociadas a otras dependencias técnicas o administrativas de la Universidad. Su equipamiento varía según su grado de implementación, y está compuesto por:

- Uno o varios equipos de usuarios especializados en los sistemas a su cargo o en los aplicativos de uso general.
- Dirigido por un coordinador/responsable, de nivel profesional con conocimientos en informática, el cual coordinará su accionar con la Dirección del Centro de Informática y Telecomunicaciones, con el fin de elaborar el **Plan Anual Estratégico de Sistemas Informáticos,** basado en la priorización e implementación de servicios informáticos, según las necesidades que las unidades operativas estipulen.

5.2 Son funciones en la implementación de un Servicio Informático las siguientes:

Todas aquellas que garantizan la real implementación y uso de un Servicio Informático, sea este implementado por el Centro de Informática y Telecomunicaciones o por un tercero:

a) **Dirección**. Conjunto de actividades que dan conducción, orientación y rumbo al Servicio Informático.

b) **Planeamiento Informático**. Consiste en la fijación de objetivos y en el desarrollo de los planes necesarios para alcanzarlos. Así mismo comprende el obtener y combinar de la forma más adecuada, los recursos humanos, materiales y financieros necesarios para la ejecución de las actividades, con el fin lograr objetivos a nivel Estratégico, Táctico y Operacional.

c) **Desarrollo**. Está compuesto por las siguientes actividades:

1. **Análisis**: Es el proceso mediante el cual se estudian e interpretan los hechos del sistema actual con el fin de encontrar los requerimientos y especificaciones funcionales del sistema a desarrollar.
2. **Diseño**: Es el proceso de definir, reemplazar o completar un sistema organizacional actual por uno informático, en dicho proceso se detalla un conjunto de especificaciones físicas que constituirán el punto de partida en la construcción del nuevo sistema informático.
3. **Programación y mantenimiento de los aplicativos, sistemas de información y bases de datos, o construcción de productos dirigidos al usuario**.

d) **Soporte**. Constituyen las actividades inherentes al manejo y mantenimiento técnico de equipos informáticos (soporte físico), así como de sus aplicativos, los sistemas de información, las bases de datos y la seguridad de los mismos (soporte lógico), que componen el Servicio Informático.

e) **Producción**. Es el manejo de los equipos y la tecnología utilizada por el Servicio Informático, con la finalidad de realizar actividades de procesamiento automático de datos y operación de sistemas de información.

f) **Apoyo y Asesoramiento a Usuarios**. Constituido por actividades de apoyo al usuario, en la elección y uso de la tecnología informática más óptima para la solución de sus problemas.

g) **Capacitación**. Es el conjunto de actividades de diseminación del conocimiento (seminarios, charlas, conferencias, etc.) sobre el uso de la tecnología informática, orientada a los usuarios del servicio.

h) **Evaluación**. Entendida como el seguimiento continuo acerca de los progresos o resultados de las actividades realizadas.

i) **Control**. Consistente en la comparación de lo avanzado en relación a lo planificado, con la finalidad de verificar si las metas deseadas se están cumpliendo. Si los resultados no están siendo alcanzados con respecto a lo planeado, se tomarán las medidas correctivas adecuadas.

5.3 **El Plan Estratégico de Sistemas de Información o Plan de Sistemas**, es el instrumento técnico que guía el desarrollo de un Servicio Informático, y debe contemplar lo siguiente:

- **La Visión Estratégica** que se tiene de la institución definiendo la misión, objetivos, metas y el ámbito del proyecto.
- **Las necesidades de información** de la institución y sus dependencias.
- **Las directrices técnicas y de gestión** que emanan de la institución.
- **El Diseño de la Arquitectura de la Información**.
- **La especificación de los nuevos sistemas**. Así como, una revisión de la situación actual de los Sistemas de Información y definir las nuevas alternativas tecnológicas.
- **Contemplar el Diseño de los Planes de Acción**, que permitan implementar el referido Plan Estratégico.

El Plan Estratégico de Sistemas de Información o Plan de Sistemas debe ser revisado periódicamente, a fin de actualizar sus objetivos, metas y alcances.

DE LA ORGANIZACIÓN DE UN SERVICIO INFORMÁTICO

5.4 Para la implementación de un servicio Informático se deberá tener en cuenta:

a) Conformar una Comisión Técnica, con personal técnico idóneo que disponga de conocimientos sobre la actividad. Dotar de facilidades adecuadas a la Comisión Técnica para el desarrollo de su misión.

b) La Comisión Técnica deberá elaborar en un plazo perentorio, un estudio de factibilidad del servicio solicitado y luego de ello, elaborar la Directiva correspondiente para su implementación, sea que ésta la realice el CIT o sea realizada por un tercero.

c) La Comisión Técnica estipulará las condiciones y elaborará mecanismos que permitan evaluar la contratación de servicios de terceros, siempre y cuando la capacidad operativa del Centro de Informática y Telecomunicaciones no se de abasto. En todo momento se toma en consideración el cumplimiento de todas las funciones de implementación de un Servicio Informático.

d) Habiéndose implementado el servicio informático, sea por el CIT o por un tercero, se deberá Institucionalizar el servicio en el organigrama funcional de la Institución, según las pautas establecidas en el Reglamento y el Manual de Organización y Funciones.

5.5 Para adecuar los Servicios Informáticos actuales a las presentes Recomendaciones Técnicas, se deberá tener en cuenta lo siguiente:

a) Conformar una Comisión Técnica para la evaluación de todos los Servicios Informáticos y la elaboración o desarrollo de un Plan Estratégico de Sistemas de Información o Plan de Sistemas que guíe a partir de ahora su desarrollo futuro.

b) El desarrollo del Plan Estratégico de Sistemas de Información o Plan de Sistemas, comprende un Análisis de los Procesos de Gestión y la Estrategia de Desarrollo Institucional, a fin de adecuar los Servicios Informáticos a esta última.

c) En el marco del referido Plan, se evaluará el nivel o etapa de desarrollo alcanzado en la actualidad y las perspectivas a futuro en el corto, mediano y largo plazo.

d) La Dirección General del Centro de Informática y Telecomunicaciones implementará los planes de acción y normatividad necesarios para orientar un adecuado servicio.

e) El Centro de Informática y Telecomunicaciones, incorporará al Plan de Trabajo Anual, un programa permanente de capacitación orientado a usuarios y a personal informático, a fin de mantener actualizado en el desarrollo de las Tecnologías de Información.

5.6 La organización de los Servicios se adecuará a la realidad institucional, en el marco de las dimensiones de la institución, la estructura organizativa y el grado de desarrollo en el tratamiento de la información**.**

DE LA EVALUACIÓN DE LAS ACTIVIDADES INFORMÁTICAS

5.7 El desarrollo e implementación de un Servicio Informático debe atravesar por varias etapas, siendo éstas las siguientes**:**

- **Primera etapa**. Comprende el período en el cual se automatizan los procesos operativos de bajo nivel para reducir los costos funcionales.
- **Segunda Etapa**. Esta etapa se caracteriza por la diseminación e interiorización de la tecnología informática por parte de los usuarios, promoviendo la automatización de procesos operativos completos.
- **Tercera Etapa**. Se caracteriza por la profesionalización de los usuarios, hay una tendencia a la administración de datos y la implicación de los usuarios en la inversión en los Servicios Informáticos.

- **Cuarta Etapa**. Se caracteriza por el desarrollo de Base de Datos y Sistemas de Información en línea, existe un mayor control administrativo y el usuario asume responsabilidades en el desarrollo del Servicio.
- **Quinta Etapa**. Se caracteriza por una orientación a la integración de los Sistemas de Información para satisfacer las necesidades de información de la institución, independientemente del entorno tecnológico (físico y lógico) que se utilice. Los usuarios son responsables en el desarrollo y uso del servicio informático (basado en sus necesidades y especificaciones).
- **Sexta Etapa**. El servicio asume el papel innovador de las Tecnologías de la Información, se desarrollan aplicaciones oportunas y competitivas. Existe una responsabilidad conjunta de usuarios e informáticos en el desarrollo del servicio.

5.8 **La Dirección del Centro de Informática y Telecomunicaciones deberá evaluar periódicamente el grado de desarrollo alcanzado, mediante el uso de técnicas apropiadas.**

DE LAS PAUTAS USADAS PARA EVALUAR LA EFICIENCIA Y EFECTIVIDAD DE UN SERVICIO INFORMÁTICO REALIZADO POR UN TERCERO

A. Nivel eficiencia:

- Tiempo necesario para el desarrollo e implementación de los proyectos informáticos. El tiempo sólo puede ser excedido según lo estipula la norma vigente.
- Evaluación Costos/Beneficios de la construcción, implementación y puesta en marcha del Servicio Informático.
- Evaluación de la productividad del equipo responsable de la construcción e implementación del servicio informático. Para ello se nombrará una Comisión de Evaluación de Productividad que tendrá como misión evaluar la productividad del Sistema Informático una vez que el mismo haya sido implementado y capacitado el personal.

B. Nivel de efectividad:

- Se evalúa la organización del Servicio informático implementado, medido a partir del control de los medios suministrados a los usuarios.
- Se evalúa el liderazgo y los procedimientos de decisión de los responsables de la construcción e implementación de los Servicios informáticos frente a la institución.
- Se evalúa el nivel de planificación que tiene el Servicio informático, de sus actividades y frente a posibles contingencias.
- Se evalúa la disponibilidad de normas y estándares establecidos y utilizados en la construcción e implementación del Servicio informático.

C. Nivel de Seguridad:

- Los Sistemas Informáticos desarrollados por terceros deberán sujetarse a las políticas de seguridad del CIT. Para ello, el CIT nombrará entre su personal, a un supervisor que realizará labores de monitoreo durante la etapa de diseño e implementación.
- El ejecutor o tercero no podrá impedir la labor de monitorización del supervisor del CIT. En caso de impedir su labor, la Universidad resolverá el contrato y se le impedirá poder ofrecer nuevamente servicios a la Universidad, de acuerdo a lo estipulado en la norma vigente.

D. Nivel de Aceptación del Sistema Informático:

- Entrega de código fuente de todas la aplicaciones, librerías y funcionalidades del sistema. Así como toda la documentación que el CIT considere necesario (diagramas, etc).

- Evaluación comparativa entre el código ejecutable entregado por ejecutor (tercero) y el ejecutable obtenido a partir del código fuente entregado por el ejecutor y compilado por el personal técnico competente del CIT.
- En caso de haber diferencia entre los códigos ejecutables del ítem anterior, el Sistema Informático no se aceptará, pudiendo la Universidad resolver el contrato con el ejecutor (tercero).

ANEXO 01

GLOSARIO DE TERMINOS

ADMINISTRACION DE DATOS

Función dentro de una organización encargada de la administración de los datos, mediante el análisis, clasificación y conservación de los datos y las relaciones entre los mismos; la coordinación para el desarrollo de modelos y diccionario de datos, combinado con el volumen de transacciones, representan la materia prima para el diseño de Base de Datos.

ARQUITECTURA DE LA INFORMACION

Concepto que describe el conjunto de estructuras que modelan el manejo de la información dentro de una organización y está compuesto por:

- Modelo conceptual de datos
- Diagrama de descomposición funcional
- Diagrama de flujo de datos
- Catálogo de funciones de la unidad
- Modelo Entidad - Relación
- Matriz Entidad - Función
- Matriz Función - Localización

AUTOEDICION

El uso de la computadora personal para producir una salida impresa de alta calidad. La autoedición requiere de un software especial, una computadora personal de alta velocidad, un monitor con presentación de página completa o de dos páginas y una impresora láser (como mínimo).

BASE DE DATOS

Conjunto de datos organizados entre los cuales existe una correlación y que están almacenados con criterios independientes de los programas que los utilizan. La filosofía de las bases de datos es la de almacenar grandes cantidades de datos de una manera no redundante y que permita los posibles consultas de acuerdo a los derechos de acceso.

DESARROLLO

Describe los procesos de Análisis, Diseño y Programación de Sistemas.

ESTUDIO DE FACTIBILIDAD

Análisis de un proyecto, que determina la posibilidad de ser realizado en forma efectiva. Los aspectos operacionales (funcionamiento), económicos (costos / beneficio) y técnicos (posible ejecución); son partes del estudio. Los resultados de un estudio de factibilidad proveen datos para una decisión de iniciar el proyecto.

MODELO DE DATOS

Es la descripción de la organización de una base de datos, constituyéndose en una representación gráfica orientada a la obtención de la estructura de datos mediante métodos.

PROCESAMIENTO AUTOMATICO DE DATOS

Se define como la actividad de captura, almacenamiento, actualización, transformación, generación y recuperación de datos por medios computacionales.

PROGRAMACION

Se define como el proceso de creación de un programa de computadora, mediante la aplicación de procedimientos lógicos mediante los siguientes pasos:

1. El desarrollo lógico mediante un algoritmo para resolver un problema en particular.
2. Escritura de la lógica del programa (algoritmo) empleando un lenguaje de programación específico (codificación del programa).
3. Ensamblaje o compilación del programa hasta convertirlo en lenguaje de máquina.
4. Prueba y depuración del programa.
5. Desarrollo de la documentación.

SEGURIDAD

Medidas de resguardo contra el acceso no autorizado a los datos. Los programas y datos se pueden asegurar entregando números de identificación y contraseñas a los usuarios autorizados de una computadora.

SERVICIO INFORMATICO

Conjunto de actividades (planeamiento, análisis, desarrollo e implementación de soluciones basadas en tecnologías de información, al nivel de hardware, software y de comunicaciones) asociadas al manejo automatizado de la información que satisfacen las necesidades y entregan valor a los usuarios de este recurso.

SISTEMA DE INFORMACION

Es el conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

SISTEMA EN LINEA (ON LINE)

Se refiere a un sistema informático que se ejecuta en dispositivos llamados terminales, sin implicar su modo de operación

Un sistema colector de datos, es un sistema en línea que acepta y almacena desde varias terminales, pero no actualiza ningún archivo maestro.

Un sistema de procesamiento de transacciones en un sistema de línea que actualiza los archivos necesarios en la medida que ingresa el trabajo, tal como en un sistema de procesamiento de órdenes de compra.

Un sistema de tiempo real es un sistema en línea que provee respuesta inmediata a un requerimiento.

USUARIO

Cualquier persona que utiliza una computadora. Por lo general se refiere a las personas que no pertenecen al personal técnico o de informática, y que proporcionan entradas y reciben salidas de los sistemas de información.

UNIVERSIDAD NACIONAL DE PIURA

CENTRO DE INFORMÁTICA Y TELECOMUNICACIONES

DIRECTIVA N°002-2015-CIT-UNP

Del uso de Antivirus en la Universidad Nacional de Piura

CIT-002 Directiva de Uso de Antivirus			
Serie:	Directiva	**Preparado por:**	Ing. Percy Casas Lazo
Versión:	1.0	**Revisado por:**	Ing. Daniel Flores Cordova
Fecha:	Agosto 2015	**Aprobado por:**	Ing. Wilfredo Cruz Yarlequé

1. INTRODUCCIÓN

Ante la creciente amenaza de virus, gusanos y otro tipo de software malicioso (*malware*) es necesario establecer una directiva que regule el uso de antivirus que vele por la seguridad de los usuarios, sistemas de información y datos de la Universidad Nacional de Piura (UNP).

Esta directiva formaliza la Política de Uso de Antivirus y establece los procedimientos que deben ser cumplidos en todos los equipos informáticos de la Universidad Nacional de Piura en toda su extensión (Campus Universitario, locales fuera del Campus Universitario y locales en sedes descentralizadas).

Un uso irresponsable de los sistemas informáticos en una dependencia no sólo afecta a los sistemas propios de ese lugar si no que puede dañar o perjudicar al resto de equipos, las aplicaciones instaladas en ellos y/o la información ahí almacenada.

1.1 Objetivo

Esta política está desarrollada para proteger los sistemas informáticos y las comunicaciones frente a virus, gusanos y otro software malicioso.

1.2 Ámbito de aplicación

El alcance de esta directiva se circunscribe a todos los equipos informáticos de la Universidad Nacional de Piura, ubicados donde quiera que éstos estén.

El Centro de Informática y Telecomunicaciones (CIT) será el ente responsable de la aplicación y cumplimiento de esta directiva en todas las dependencias de la UNP.

2. ANTIVIRUS CORPORATIVO

La solución corporativa de seguridad de antivirus es una solución integrada de herramientas antivirus, antispyware, firewall y prevención contra intrusiones, además del control de dispositivos y aplicaciones usando un único agente multiplataforma (Windows, Mac, Linux) para todos los usuarios y gestionado mediante una consola central con motor de base de datos.

Complementando el servicio antivirus se ha implementado el repositorio central de actualización para toda la plataforma antivirus, facilitando la gestión de descarga y distribución de actualizaciones, permitiendo que todos los equipos de la UNP tengan las últimas versiones y parches emitidos por el fabricante.

Los equipos integrados en el dominio de la UNP tienen instalado un antivirus corporativo gestionado en forma centralizada por el CIT y que se actualiza automáticamente de forma periódica. Sin embargo, en los computadores ubicados fuera del Campus Universitario se instalará el antivirus corporativo de forma local ("*off line*") de manera sencilla por personal del CIT o personal que labora en dichos locales.

Los usuarios locales de estos equipos dispondrán de cartillas (en físico y en la web) para su eficiente manejo.

3. POLÍTICA DE ANTIVIRUS

3.1 Instalación de antivirus

Todos los computadores deben ejecutar una versión actualizada del software antivirus proporcionado local o remotamente por el CIT. Este software es capaz de proteger al sistema operativo y a las aplicaciones en tiempo real, y de actualizarse de forma automática cada vez que se conecte un computador a la red de datos de la Universidad.

Todos los equipos de cómputo de la Universidad Nacional de Piura deben tener instalado el antivirus proporcionado por el CIT, para lo cual se llevará un registro de todos los equipos, sean éstos de escritorio (desktop) o portátiles (laptop) .

La desinstalación de la aplicación se encuentra restringida a la validación de clave de desinstalación. Cualquier proceso de desinstalación no autorizado podría dañar no sólo el equipo sino también a las aplicaciones e información contenidas en él.

El proceso de desinstalación del antivirus requiere la aprobación del Director General del CIT previa explicación de motivos.

Cualquier antivirus que no sea el proporcionado por el CIT y que se encuentre instalado en cualquier computadora perteneciente a la Universidad será desinstalado y removido de forma local o remota, no haciéndose el CIT responsable de los daños ocasionados por esta acción. La reiteración del hecho de instalar antivirus no autorizados será considerado una falta grave y se informará a la autoridad para las sanciones correspondientes.

3.2 De las responsabilidades del Centro de Informática y Telecomunicaciones

El Centro de Informática y Telecomunicaciones de la UNP (CIT) implementará el antivirus en todas las computadoras de la Universidad.

El CIT solucionará contingencias presentadas ante el surgimiento de virus que la solución no se haya detectado automáticamente.

La configuración del analizador de red para la detección de virus es responsabilidad exclusiva del CIT. La definición de las políticas contra virus y otros tipos de ataques es potestad del CIT dentro del marco de la Política de Seguridad de la Información de la UNP.

El CIT aislará el equipo o red, notificando a la autoridad, en las condiciones siguientes:

- Cuando la contingencia con virus no es controlada, con el fin de evitar la propagación del virus a otros equipos y redes.
- Si el usuario viola las políticas antivirus dispuestas en esta directiva.
- Cada vez que los usuarios requieran hacer uso de discos, USBs, éstos serán rastreados por la aplicación antivirus en la computadora del usuario o en un equipo designado para tal efecto en

las áreas de cómputo de las dependencias.

3.3 Protección ininterrumpida

Mientras el computador esté conectado a la red de la Universidad, no se debe detener, en ningún caso, la ejecución del antivirus, porque se perdería la protección del computador y la actualización del antivirus.

El antivirus se ha programado para realizar una vez por semana una inspección integral del sistema (disco y memoria, principalmente). Durante ese lapso, el equipo no deberá apagarse.

Periódicamente, además del rastreo en los equipos de cómputo, se realizará la actualización de las firmas de antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la red de la UNP.

El CIT estará en permanente monitoreo de los equipos en la red.

3.4 Eliminación de virus

Cuando se sospeche de una infección o cuando el antivirus detecte una, se procederá a su limpieza de manera automática. En caso de no poder realizarse esta limpieza, el antivirus emitirá una alerta por lo que se debe contactar con el CIT (anexo 8527) para su realización por personal debidamente autorizado.

En caso de que el virus comienza a ocasionar daños en el sistema se deber reportar de inmediato al CIT (anexo 8527).

3.5 Políticas Antivirus

Utilizando la consola de administración se implementan las siguientes políticas:

- **Virus y Spyware**

Acción	Frecuencia	Computadoras de escritorio	Computadoras portátiles	Servidores
Scaneo base	Diario, 1:00 PM	Si	Si	No
Scaneo completo	Jueves, 11:00 AM	Si	Si	Si
Actualizaciones	Diario	Si	Si	Si

- **Autoprotect**

Descripción	Tipo de detección	Primera acción	Segunda acción (de fallar la primera)
Revisión Automática de todos los archivos. Riegos de Seguridad, Equipos remotos cuando se ejecutan archivos.	Malware/Antivirus	Limpiar	Borrar
	Riegos de seguridad	Borrar	Cuarentena

- **Descargas**

Descripción	Tipo de detección	Primera acción	Segunda acción (de fallar la primera)
Análisis de Riegos potenciales basados en reputación con nivel de sensibilidad intermedia, que permite tener un numero bajo de falsos positivos sin comprometer el desempeño de los computadores	Archivos maliciosos	Borrar	Cuarentena
	No probados	Sugerir	No aplica

- **Protección proactiva de amenazas**

Acción	Tipo de detección	Alto riesgo	Bajo riesgo
Protección Proactiva de amenazas	Amenaza	Log	Log
	Eventos de cambio: DNS, HOST FILE	Log	Log
	Comportamiento Sospechoso	Bloqueo	No aplica

- **Autoprotect Mail**

Servicios	Descripción	Tipo detección	Primera acción	Segunda acción
Internet mail	Scan de todos los archivos y hasta tres niveles de compresión	Malware/Antivirus	Limpiar	Borrar
		Riegos de seguridad	Borrar	Cuarentena
Microsoft Outlook, Lotus Notes y otros	Se encuentra desactivada esta opción por no usar ninguna plataforma de correo cliente con servidor local. Nuestro servicio es un servicio web basado en Google Apps con sus propias políticas de seguridad y control. Adicionalmente servicios de correo basados en POP e IMAP se encuentra restringidos en LAN. Los usuario no podrán instalar servicios de correo en la red de la Universidad			

- **Firewall**
  - Desactiva el firewall de Windows y establece políticas de reglas centralizadas
  - Veintiséis reglas preestablecidas en la instalación y que son recomendación de buenas prácticas por el fabricante
  - Servicios como DHCP, DNS y WINS son controlados por tráfico desde la herramienta. Los usuarios no podrán instalar estos servicios en la red de la Universidad.

- **Intrusion Prevention**
  - Detecta y bloquea automáticamente ataques de red y a navegadores de Internet. Permanece activada globalmente

- **Control de Aplicaciones y Dispositivos**
  - Conjunto de reglas que permiten controlar acceso de aplicaciones y/o dispositivos a los

recursos del sistema, con el fin de prevenir riesgos de infección y/o seguridad; no se bloqueará el acceso a dispositivos como CD/DVD-ROM, USB o discos externos.

- Bloqueo a ejecución de aplicaciones desde CD-ROM/DVD-ROM y dispositivos de almacenamiento removibles incluyendo Autorun.Inf
- Limitaciones a la copia de documentos oficiales en dispositivos como USB, CD-ROM, discos duros externos, etc. Esta política restringirá el hecho de copiar archivos en cuyo contenidos se incluya las palabras "Universidad Nacional de Piura", "Resolución", y otras que la autoridad considere apropiado.

- **Uso del Antivirus por los usuarios**
  - El usuario no deberá desinstalar la aplicación antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.
  - Si el usuario hace uso de medios de almacenamiento personales, éstos deberán ser rastreados por la aplicación antivirus en la computadora del usuario o por el equipo designado para tal efecto.
  - El usuario deberá comunicarse con el CIT en caso de problemas de virus para buscar la solución.
  - El usuario será notificado por el CIT en los siguientes casos:
    - Cuando sea desconectado de la red con el fin evitar la propagación del virus a otros usuarios de la dependencia.
    - Cuando sus archivos resulten con daños irreparables por causa de virus.
    - Cuando viole las políticas antivirus.

3.6 Creación o difusión de software malicioso

En ningún caso, incluido cualquier fin académico, los usuarios pueden escribir, compilar, copiar, propagar o ejecutar de forma intencionada en equipos que se conecten a la red de datos de la Universidad código diseñado para replicarse, dañar, espiar o entorpecer el desempeño de cualquier sistema operativo, aplicación informática o de comunicaciones.

3.7 Incumplimiento

El incumplimiento de esta directiva puede acarrear la revocación de privilegios de acceso o el bloqueo del equipo. La autoridad será informada de este tipo de sucesos para las sanciones correspondientes.